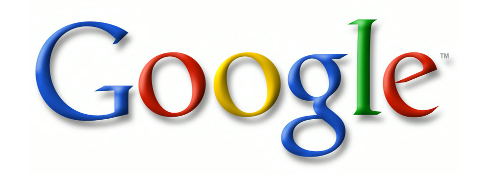



Hosted by Google

ZAHLENTHEORIE

VON

ADRIEN-MARIE LEGENDRE.

NACH DER
DRITTEN AUFLAGE INS DEUTSCHE ÜBERTRAGEN

VON

H. MASER.

ERSTER BAND.

LEIPZIG
DRUCK UND VERLAG VON B. G. TEUBNER.
1886.

LIPSIAE: TYPIS B. G. TEUBNERI.

Vorwort des Übersetzers.

In der Infinitesimalrechnung begegnet man sehr häufig der Erscheinung, dafs Sätze, welche früher allgemein als richtig anerkannt wurden, plötzlich angefochten oder gar umgestofsen werden. Diese Erscheinung hat ihren Grund hauptsächlich darin, dafs die begrifflichen Grundlagen im Laufe der Zeit schärfer definiert werden und eine klarere Anschauung über das eigentliche Wesen derselben Platz greift. (Um ein Beispiel anzuführen, erinnere ich nur an den Cauchy'schen Irrtum, dafs die Stetigkeit einer Funktion zum Beweise ihrer Differenziierbarkeit genüge, sowie an die noch heute nicht endgültig gelöste Streitfrage über die Darstellbarkeit willkürlicher Funktionen durch trigonometrische Reihen). Die höchst einfachen und wenigen Grundbegriffe der Zahlentheorie sind dagegen unveränderlich, es bleiben daher auch die einmal bewiesenen Eigenschaften der Zahlen für alle Zeiten unumstöfsliche Wahrheiten. Während somit die Fortbildung der Analysis vor Allem durch eine präcisere Bestimmung ihrer Begriffe und tiefere Erkenntnis ihrer Grundlagen bedingt ist, hängt die weitere Entwicklung der Zahlentheorie hauptsächlich von der Ausbildung ihrer Methoden und davon ab, ob es gelingt, für möglichst viele Eigenschaften der Zahlen eine gemeinsame Quelle aufzufinden. Daher kommt es, dafs ältere die Analysis behandelnde Werke in späterer Zeit sehr häufig nur noch historischen Wert besitzen, Werke aber, welche der Zahlentheorie gewidmet sind, im eigentlichen Sinne für das Studium nie unbrauchbar werden können. Letzteres dürfte auch der Grund sein, weshalb es nur sehr wenige, aber um so bedeutendere, ausführliche Werke giebt, welche die Lehre von den Eigenschaften der Zahlen zum Gegenstande haben.

Für die Entwicklung der Zahlentheorie hat unstreitig Gauss bisher das Bedeutendste geleistet. Durch sein unsterbliches Werk

„Disquisitiones arithmeticae" erhob er die Lehre von den Eigenschaften der ganzen Zahlen aus der Finsternis, in der sie nach Fermat ein Jahrhundert lang gelegen hatte und in der sie nur durch einige Strahlen von Sternen erster Gröfse gestreift worden war, mit einem Schlage zu dem vollen Glanze einer ausgebildeten Wissenschaft. Neben ihm aber hat Legendre Anspruch auf den ersten Platz. Nachdem derselbe in mehreren Abhandlungen wertvolle Beiträge zur tieferen Erkenntnis der Natur der Zahlen geliefert hatte, gab er in seinem nur wenige Jahre vor den Gauss'schen Untersuchungen erschienenen Werke „Essai sur la théorie des nombres" eine Zusammenstellung aller bis dahin bekannten, teils von andern Gelehrten, teils von ihm selbst entdeckten Eigenschaften der Zahlen. Das quadratische Reciprocitätsgesetz, das „Theorema fundamentale", wie es Gauss nennt, bildet den Glanzpunkt seiner Entdeckungen auf diesem Gebiete. Im Jahre 1808 folgte eine zweite und 1830 eine dritte, stark vermehrte Auflage desselben Werkes, welche auch den Gauss'schen Entdeckungen zum Teil Rechnung trug.

Bei dem Mangel an Werken, welche die Theorie der Zahlen behandeln, und wegen der eigenartigen Schwierigkeiten, welche das Studium der Disquisitiones besonders dem Anfänger bereitet, Schwierigkeiten, die beim Legendre'schen Werke bei Weitem nicht so grofs sind, wird man hoffentlich eine neue Ausgabe dieses letzteren in deutscher Sprache nicht ungern sehen, zumal auch die Beschaffung des Originals wegen der Seltenheit desselben fast Jedermann unmöglich geworden ist.

Die Übersetzung hält sich streng an den Wortlaut des Originals, damit man dieses um so weniger vermisse. Berichtigende oder erläuternde Anmerkungen sind absichtlich nicht hinzugefügt worden; ich halte es geradezu für unschicklich, wenn man, wie es oft genug geschieht, durch eine solche vom heutigen Standpunkte der Wissenschaft aus gefällte mehr oder minder zutreffende Kritik auch nur den Schein erweckt, als ob man sagen wolle, der betreffende Autor hätte seine Sache besser machen können. Allerdings ist die Art, wie Legendre die Eigenschaften der Zahlen ableitet und die darauf bezüglichen Sätze ausspricht, überhaupt seine Auffassung der Zahlentheorie als unbestimmte Analysis von der heute üblichen, durch Gauss begründeten Behandlungsweise etwas verschieden, so dafs vielleicht ein kurzer Hinweis auf die Verschiedenartigkeit der Anschauungen für den Anfänger am Platze gewesen wäre. Ich habe aber auch diesen unterlassen, da der Vortrag Legendre's so klar und durchsichtig ist, dafs

jeder sehr bald selbst herausfinden wird, worin jene Verschiedenheiten beruhen.

Offenbare Druckfehler des Originals habe ich dagegen ohne Weiteres verbessert und mich bemüht, durch Hervorheben einzelner Worte oder ganzer Sätze sowie durch die Stellung der Formeln die Übersicht über den Inhalt soviel wie möglich zu erleichtern.

Möge denn diese deutsche Ausgabe von Legendre's „Théorie des nombres“ an ihrem Teile zur Förderung des Studiums der Zahlentheorie beitragen helfen.

Berlin, im Januar 1886.

H. Maser.

Vorwort (des Verfassers) zur dritten Ausgabe.

Diese Ausgabe unterscheidet sich von der vorigen sowohl durch einige verbessernde Zusätze, wie durch eine neue Einteilung des Stoffes; jedoch ist der gröfste Teil der vorgenommenen Änderungen, um den Zusammenhang des Werkes nicht zu stören, an das Ende desselben gesetzt worden.

Es haben daher die drei ersten Hauptteile, welche den ersten Band dieser Ausgabe bilden, nur geringfügige Änderungen erfahren; dagegen enthält der vierte Hauptteil, mit welchem der zweite Band beginnt, am Schlusse eine grofse Menge von Zusätzen. Der fünfte Hauptteil ist fast vollständig umgearbeitet worden; man findet darin neue sehr umfassende Untersuchungen über die von Gauss für die Auflösung der binomischen Gleichungen angegebenen Methoden.

Der sechste Hauptteil und der darauf folgende Anhang sind an die Stelle der beiden Supplemente getreten, welche der zweiten Ausgabe beigegeben waren; sie bieten übrigens den Mathematikern mehrere Beweise und Lösungen von Aufgaben, die ich bisher noch nicht veröffentlicht habe.

Nachdem das Werk auf diese Weise alle Vervollkommnungen erfahren hat, welche der Verfasser vermöge seiner eigenen Untersuchungen und mit Benutzung der Arbeiten anderer Mathematiker ihm geben konnte, schien es angemessen, den bisherigen Titel des Werkes „Versuch einer Theorie der Zahlen“ endgültig in den Titel „Zahlentheorie“ umzuändern.



Der Verfasser verhehlt sich nicht, dafs manche der in diesem Werke behandelten Gegenstände der Vervollständigung oder selbst Berichtigung durch neue Untersuchungen bedürfen; er ist jedoch der Ansicht, dafs es besser sei, sie in diesem Zustande der Unvollkommenheit zu lassen, als sie vollständig zu unterdrücken. Sie bieten ein passendes Arbeitsfeld für diejenigen, welche sich fernerhin der Vervollkommnung der Wissenschaft widmen wollen.

Vorwort (des Verfassers) zur ersten Ausgabe.

Nach den verschiedenen Bruchstücken zu urteilen, die auf uns gekommen und von denen einige im Euclid angeführt sind, scheinen die alten Philosophen ziemlich ausgedehnte Untersuchungen über die Eigenschaften der Zahlen angestellt zu haben. Zur gründlicheren Erforschung dieser Wissenschaft fehlten ihnen indessen zwei Hülfsmittel: die ziffermäfsige Darstellung, welche dazu dient die Zahlen mit grofser Leichtigkeit auszudrücken, und die Algebra, welche die Resultate verallgemeinert und in gleicher Weise mit bekannten und unbekannten Gröfsen rechnet. Die Erfindung dieser beiden Künste mufste daher auf die weitere Entwicklung der Wissenschaft von den Zahlen bedeutenden Einflufs üben. So sieht man denn, dafs das ganze Werk des Diophant von Alexandria, der, soweit bekannt, der älteste Autor ist, welcher über Algebra geschrieben, von den Eigenschaften der Zahlen handelt und schwierige Aufgaben enthält, die mit grofser Geschicklichkeit und vielem Scharfsinn gelöst sind.

Von Diophant bis zur Zeit Vieta's und Bachet's fuhren die Mathematiker zwar fort, sich mit den Zahlen zu beschäftigen, jedoch ohne grofsen Erfolg, und ohne die Wissenschaft merklich zu fördern.

Vieta, welcher die Algebra weiter vervollkommnete, löste mehrere schwierige, auf die Zahlen bezügliche Probleme. Bachet gab in seinem Werke: „Problèmes plaisans et délectables“ eine allgemeine und sehr geistreiche Methode für die Auflösung der unbestimmten Gleichungen ersten Grades. Demselben Gelehrten verdanken wir einen ausgezeichneten Commentar zum Diophant, welcher später durch Randbemerkungen von Fermat bereichert wurde.

Fermat, einer der Geometer, durch deren Arbeiten die Entdeckung der neuen Rechnungsarten am meisten beschleunigt wurde,

beschäftigte sich sehr erfolgreich mit der Wissenschaft der Zahlen und brach derselben neue Bahnen. Wir verdanken ihm eine grofse Menge von merkwürdigen Sätzen, die er jedoch fast alle ohne Beweis gelassen hat. Es lag im Geiste der Zeit, sich gegenseitig Aufgaben zu stellen; man verheimlichte dabei meistens seine eigene Auflösungsmethode, um sich und seiner Nation neue Triumphe vorzubehalten. Eine solche Rivalität bestand besonders zwischen den französischen und englischen Mathematikern. Daher ist es gekommen, dafs die meisten Beweise Fermat's verloren gegangen sind; die wenigen, die auf uns gekommen sind, lassen uns umsomehr die uns fehlenden vermissen.

Von Fermat bis auf Euler gaben sich die Mathematiker, vollständig mit der Entdeckung oder Anwendung der neuen Rechnungsarten beschäftigt, nicht mit der Theorie der Zahlen ab. Euler nahm sich zuerst wieder dieses Teils der mathematischen Wissenschaften an. Die zahlreichen Abhandlungen, die er hierüber in den Abhandlungen der Petersburger Akademie und in andern Werken veröffentlicht hat, liefern den Beweis, wie sehr es ihm am Herzen lag, der Wissenschaft der Zahlen dieselbe Förderung angedeihen zu lassen, welche die meisten andern Teile der Mathematik ihm verdanken. Ja man kann sagen, dafs Euler einen besonderen Gefallen an derartigen Untersuchungen hatte und sich ihnen mit einer gewissen Leidenschaft hingab, wie es fast bei allen der Fall ist, die sich mit der Zahlentheorie beschäftigen. Wie dem auch sein möge, seine Untersuchungen führten ihn zum Beweise zweier Hauptsätze Fermat's, nämlich 1) dafs, wenn a eine Primzahl und x eine beliebige, durch a nicht teilbare Zahl ist, die Formel $x^{a-1}-1$ stets durch a sich teilen läfst, 2) dafs jede Primzahl von der Form $4n+1$ die Summe zweier Quadrate ist.

Eine Menge anderer wichtiger Entdeckungen sind in den Abhandlungen Euler's enthalten. Man findet darin die Theorie der Teiler der Gröfse $a^n \pm b^n$; die Abhandlung über die Zerlegung der Zahlen in Teile, welche auch in seine „Einleitung in die Analysis des Unendlichen“ aufgenommen ist; die Anwendung der imaginären und irrationalen Faktoren bei der Auflösung der unbestimmten Gleichungen; die allgemeine Auflösung der unbestimmten Gleichungen zweiten Grades unter der Voraussetzung, dafs man eine specielle Lösung kenne, den Beweis vieler Sätze über die Potenzen der Zahlen, und besonders den zweier von Fermat angegebenen Sätze, dafs die Summe oder Differenz zweier Kuben kein Kubus, und die Summe oder Differenz zweier Biquadrate kein Quadrat sein kann. Endlich findet

man in diesen Schriften eine grofse Menge unbestimmter Aufgaben, welche durch sehr geistreiche analytische Kunstgriffe gelöst sind.

Euler ist lange Zeit hindurch fast der einzige Mathematiker gewesen, der sich mit der Zahlentheorie beschäftigte. Endlich trat Lagrange auch auf dieses Gebiet über; seine ersten Schritte waren von Erfolgen begleitet, gleich denen, welche er bereits bei Untersuchungen höherer Art errungen hatte. Eine allgemeine Methode, die unbestimmten Gleichungen zweiten Grades aufzulösen, und was noch schwieriger war, eine Methode, sie in ganzen Zahlen aufzulösen, war der erste Versuch dieses berühmten Gelehrten. Bald darauf wandte er die Kettenbrüche auf diesen Zweig der Analysis an; er bewies zuerst, dafs der Kettenbruch, welcher gleich der Wurzel einer rationalen Gleichung zweiten Grades ist, periodisch sein mufs, und schlofs daraus, dafs das auf die Gleichung $x^2 - Ay^2 = 1$ bezügliche Fermat'sche Problem immer lösbar ist, ein Satz, der bis dahin noch nicht in strenger Weise begründet war, obwohl mehrere Mathematiker Methoden für die Auflösung dieser Gleichung gegeben hatten.

Derselbe Gelehrte bewies in seinen weiteren Untersuchungen, welche in den Abhandlungen der Berliner Akademie niedergelegt sind, zuerst den Satz, dafs jede ganze Zahl die Summe von vier Quadraten ist; ebenso verdanken wir ihm mehrere andere wichtige Beweise. Die bemerkenswerteste aller seiner Entdeckungen ist indessen eine allgemeine Methode, aus der sich eine unendliche Menge von Sätzen über die Primzahlen als unmittelbare Folgerungen ergeben.

Diese aufserordentlich fruchtbare Methode gründet sich auf die Betrachtung sowohl der quadratischen wie der linearen Formen, welche den Teilern der Formel $t^2 + au^2$, in welcher t und u zwei unbestimmte Gröfsen sind und a eine gegebene Zahl bedeutet, zukommen. Es blieb jedoch noch der allgemeine Beweis der Relation zu führen übrig, welche zwischen den linearen und den quadratischen Formen bei den Primzahlen bestehen mufs. Denn in Ermangelung eines allgemeinen, diese Relation*) enthaltenden Prinzips liefert die Lagrange'sche Theorie zwar unendlich viele Sätze für die Primzahlen von der Form $4n + 3$, aber nur eine geringe Anzahl für die Primzahlen von der Form $4n + 1$.

Eine Abhandlung, welche ich in dem Bande der Akademie der Wissenschaften für das Jahr 1785 veröffentlichte, giebt die Hülfs-

*) Siehe hierüber die Abhandlungen der Akademie der Wissenschaften zu Berlin vom Jahre 1775 Seite 350 u. 352. Anm. d. Verf.

mittel zum Beweise des erwähnten Prinzips an die Hand und enthält überdies Sätze, vermittelst deren eine weitere Entwicklung der Zahlentheorie möglich werden dürfte. Ich habe darin gegeben 1) den Beweis eines Satzes, mit dessen Hülfe die Möglichkeit oder Unmöglichkeit einer jeden, auf die Form $ax^2 + by^2 = cz^2$ gebrachten unbestimmten Gleichung zweiten Grades festgestellt werden kann; 2) den Beweis eines allgemeinen Gesetzes, welches zwischen zwei beliebigen Primzahlen besteht und „das Reciprocitätsgesetz" genannt werden kann; 3) die Anwendung dieses Gesetzes auf verschiedene Sätze und den Gebrauch desselben sowohl zur Vervollkommnung der Theorie von Lagrange wie zur Beseitigung von andern Schwierigkeiten derselben Art.

Die nämliche Abhandlung enthält ferner den Entwurf einer vollständig neuen Theorie der Zahlen, insofern dieselben als in drei Quadrate zerlegbar betrachtet werden. Dieser Theorie gehört der berühmte Fermat'sche Satz an, dafs eine beliebige Zahl die Summe von drei Trigonalzahlen ist, und ferner der Satz desselben Autors, dafs jede Primzahl von der Form $8n + 7$ die Form $p^2 + q^2 + 2r^2$ besitzt.

Seit der Veröffentlichung dieser Abhandlung habe ich die Entwicklung der darin enthaltenen Gesichtspunkte wiederholentlich überarbeitet und verschiedene Punkte der Theorie der Zahlen oder der unbestimmten Analysis*) zu vervollkommnen gesucht. Da meine Untersuchungen in dieser Hinsicht von einigem Erfolge begleitet waren, so war es zunächst meine Absicht, das Resultat derselben in einer besonderen Abhandlung zu veröffentlichen; später jedoch glaubte ich diese Gelegenheit benutzen zu müssen, um die Theorie der Zahlen mit gröfserer Ausführlichkeit, als dies bisher geschehen, zu behandeln, indem ich das Ergebnis der hauptsächlichsten, auf denselben Gegenstand bezüglichen Untersuchungen von Euler und Lagrange mit meinen eigenen zusammenfafste.

Aus diesem Grunde habe ich mich entschlossen, das Werk, wel-

---

*) Ich trenne die Theorie der Zahlen und die unbestimmte Analysis nicht von einander, sondern betrachte diese beiden Teile als einen einzigen Zweig der algebraischen Analysis. Denn es giebt keinen Satz über die Zahlen, der sich nicht auf die Auflösung einer oder mehrerer unbestimmten Gleichungen bezöge. Wenn man z. B. mit Fermat behauptet, dafs jede Primzahl von der Form $4n + 1$ die Summe zweier Quadrate ist, so ist dies dasselbe, als ob man sagt: Die Gleichung $A = y^2 + z^2$ ist stets auflösbar, sobald die Zahl A eine Primzahl von der Form $4n + 1$ ist. Man könnte hinzufügen, dafs in eben diesem Falle die Gleichung $A = y^2 + z^2$ stets nur eine Lösung besitzt. Dies ergäbe einen zweiten Satz, welcher eine charakteristische Eigenschaft der Primzahlen von der Form $4n + 1$ enthielte. Anm. d. Verf.



ches ich hiermit der Öffentlichkeit übergebe, zusammenzustellen. Ich betrachte es nicht als ein den Gegenstand erschöpfendes Werk, sondern nur als einen Versuch, welcher ungefähr den gegenwärtigen Stand der Wissenschaft zeigen und vielleicht dazu beitragen kann, die weitere Entwicklung derselben zu beschleunigen. [Es kommt mir nicht zu, noch mehr über mein eigenes Werk zu sagen, nur das will ich noch hinzufügen, dafs ich nichts aufser Acht gelassen habe, um es der Aufmerksamkeit der Mathematiker würdig zu machen. Aber welche Sorgfalt ich auch auf die Untersuchung der verschiedenen besondern Fälle mehrerer Sätze verwandt habe, ich fühle, dafs manche Lücken geblieben und vielleicht sogar Irrtümer mit untergelaufen sind. Vor allem zweifle ich nicht, dafs mehrere der neuen Sätze, die ich nur mit vieler Mühe begründen konnte, auf weit einfachere Weise bewiesen werden können, sei es mit Hülfe noch unbekannter Principien, sei es durch Beziehungen, die ich nicht bemerkt habe. Wie dem auch sein möge, ich schmeichle mir, dafs die Mathematiker, in Erwägung der Schwierigkeiten und der Neuheit des Stoffes, diese Versuche mit Nachsicht aufnehmen werden, und ich hoffe, dafs auch die Fehler, in die ich verfallen bin, zum Nutzen der Wissenschaft ausschlagen werden, indem sie geschickteren Händen Gelegenheit geben, denselben Gegenstand zu behandeln und ihn zu einer gröfseren Vollkommenheit zu führen*)].

*) Die hier in Parenthese eingeschlossenen Worte des Vorwortes zur ersten Ausgabe sind in der dritten Ausgabe weggelassen. Anm. d. Übers.

Inhaltsverzeichnis zum ersten Bande.

Einleitung,
Allgemeine Sätze über die Zahlen enthaltend.

Erster Hauptteil.
Entwicklung von verschiedenen Methoden und Sätzen, welche sich auf die unbestimmte Analysis beziehen.





Zweiter Hauptteil.

Allgemeine Eigenschaften der Zahlen.

Dritter Hauptteil.

Theorie der Zahlen, insofern sie sich in drei Quadrate zerlegen lassen.



Tafeln.

Einleitung,

Allgemeine Sätze über die Zahlen enthaltend.

In dieser Einleitung werden wir einige allgemeine Betrachtungen über die Natur der Zahlen und insbesondere über die der Primzahlen anstellen. Vor Allem aber halten wir es für notwendig, uns mit einigen fundamentalen Sätzen zu beschäftigen, deren Beweis in den gewöhnlichen Lehrbüchern der Arithmetik sich entweder gar nicht findet oder wenigstens nicht mit der nötigen Strenge gegeben wird.

I.

Wir untersuchen zuerst, warum das Produkt zweier Zahlen, wenn man die Reihenfolge der Faktoren ändert, dasselbe bleibt, d. h. warum $A \times B = B \times A$ ist.

Ist A die gröſsere der beiden Zahlen A und B, und C ihre Differenz, folglich $A = B + C$, so wird man ohne Weiteres zugeben, daſs das Produkt aus A und B, d. h. A B-mal genommen, sich aus dem Produkt von B und B und dem Produkt von C und B zusammensetzt, so daſs man, wenn man den Multiplikator zuletzt schreibt,

$$A \times B = B \times B + C \times B$$

hat. Das Produkt aus B und A oder $B + C$ ist aber ebenfalls aus B B-mal genommen und aus B C-mal genommen zusammengesetzt, so daſs

$$B \times A = B \times B + B \times C$$

ist. Daraus erhellt, daſs das Produkt $A \times B$ dasselbe sein wird wie das Produkt $B \times A$, wenn das Teilprodukt $C \times B$ gleich $B \times C$ ist. In derselben Weise aber folgert man die Gleichheit zwischen CB und BC aus der Gleichheit zweier kleineren Produkte CD und DC, und fährt man so fort, so gelangt man notwendig entweder zu dem Falle, wo die beiden Faktoren gleich sind, oder zu dem, wo der eine von

beiden gleich der Einheit ist. Im ersteren Falle ist die Gleichheit augenscheinlich; in dem zweiten folgt sie daraus, dafs $H \times 1$ ebenso wie $1 \times H$ gleich H ist. Mithin ist das Produkt $A \times B$ stets gleich dem Produkte $B \times A$.

II.

Man setzt in der Regel voraus, dafs es, wenn man eine Zahl C mit einer andern Zahl N, welche selbst das Produkt zweier Faktoren A und B ist, multiplicieren soll, gleichgültig ist, ob man C sogleich mit dem ganzen Produkte N, oder erst C mit A und sodann das Produkt mit B multipliciert.

Um die Richtigkeit dieses Satzes darzuthun, bemerke man zunächst, dafs das Produkt AB nichts anderes ist als: $A + A + A + \cdots$, wobei die Anzahl dieser Glieder gleich B ist. Multipliciert man demnach eine dritte Zahl C mit dem Produkte AB, so hat man die Operation der Multiplikation von C mit A B-mal zu wiederholen, d. h. man erhält $CA + CA + CA + \cdots$, wobei das Glied CA B-mal zu setzen ist. Das Resultat ist also $CA \times B$, so dafs man hat:

$$C \times AB = CA \times B.$$

III.

Auf Grund dieser beiden Sätze zeigt man leicht, dafs das Produkt beliebig vieler Faktoren stets dasselbe bleibt, in welcher Reihenfolge man auch die Faktoren mit einander multiplicieren möge.

Soll z. B. bewiesen werden, dafs das Produkt $A \times B \times C \times D$ gleich dem Produkte $C \times A \times D \times B$ ist, so bringe man zunächst in beiden Produkten denselben Buchstaben an die letzte Stelle. Nach den vorhergehenden Sätzen hat man nämlich:

$$A \times BC = A \times CB = AC \times B,$$

mithin:

$$A \times B \times C \times D = AC \times B \times D = AC \times BD = AC \times D \times B.$$

In diesem Produkte steht der Buchstabe B an der letzten Stelle, ebenso wie in dem andern gegebenen Produkte $CADB$. Läfst man jetzt den letzten Buchstaben weg, so hat man nur noch die Gleichheit

$$AC \times D = C \times A \times D$$

zu beweisen, und diese ergiebt sich daraus, dafs $AC = C \times A$ ist.

IV.

Das **Produkt zweier** Zahlen A und B ist durch jede Zahl **teilbar**, welche in einem der beiden Faktoren A und B genau aufgeht.

Denn ist ϑ eine Zahl, welche in B aufgeht, und ist somit $B = C \times \vartheta$, so erhält man $AB = AC \times \vartheta$. Mithin giebt AB, durch ϑ geteilt, den genauen Quotienten AC.

V.

Wenn die Zahl ϑ gleichzeitig in den beiden Zahlen A und B genau aufgeht, so geht sie auch in der **Summe** und **Differenz** von zwei beliebigen Vielfachen dieser Zahlen auf.

Denn ist $A = A'\vartheta$, $B = B'\vartheta$, so erhält man:

$$mA \pm nB = mA'\vartheta \pm nB'\vartheta,$$

also eine Grösse, welche durch ϑ geteilt den genauen Quotienten $mA' \pm nB'$ giebt.

VI.

Eine **Primzahl**, welche in keinem der beiden Faktoren A und B aufgeht, kann auch kein Teiler ihres Produkts AB sein.

Da **dieser Satz einer der wichtigsten** in der Zahlentheorie ist, so wollen wir den Beweis desselben in aller Ausführlichkeit entwickeln.

Gäbe es wirklich eine Primzahl ϑ, welche keine der beiden Zahlen A und B, wohl aber ihr Produkt AB teilt, so könnte man annehmen, daſs sich bei der Division von A durch ϑ der Quotient m (welcher auch gleich 0 sein könnte) und der Rest A' ergebe. Man würde also

$$A = m\vartheta + A'$$

und ebenso

$$B = n\vartheta + B'$$

folglich

$$AB = mn\vartheta^2 + nA'\vartheta + mB'\vartheta + A'B'$$

erhalten. Diese Grösse müsste unserer Annahme entsprechend durch ϑ teilbar sein, und da die drei ersten Glieder durch ϑ teilbar sind, so müsste sich auch das vierte Glied durch ϑ teilen lassen. Man könnte also setzen:

$$A'B' = C'\vartheta.$$

Zu diesem ersten Resultat bemerken wir:

1) daſs von den Zahlen A' und B' keine gleich 0 sein kann, da A und B nach Voraussetzung nicht durch ϑ teilbar sind;

2) dafs A' und B', als Reste der Division durch ϑ, kleiner sind als ϑ;

3) dafs keine der Zahlen A' und B' gleich der Einheit sein kann. Hätte man nämlich $A' = 1$, so würde sich das Produkt $A'B'$ auf B' reducieren, und da $B' < \vartheta$ ist, so könnte unmöglich $B' = C'\vartheta$ sein.

Man hätte also zwei ganze Zahlen A', B', welche beide grösser als 1, aber kleiner als ϑ sind, und deren Produkt durch ϑ sich teilen liefse, so dafs

$$A'B' = C'\vartheta$$

wäre. Sehen wir zu, welche Folgerungen sich daraus ergeben würden.

Da A' kleiner ist als ϑ, so kann man ϑ durch A' dividieren; ist p der Quotient und A'' der Rest, so erhält man:

$$\vartheta = pA' + A''$$

folglich:

$$\vartheta \times B' = pA'B' + A''B'.$$

Da die linke Seite dieser Gleichung durch ϑ teilbar ist, so muss es auch die rechte sein. Da ferner $A'B' = C'\vartheta$, und demnach der Teil $A'B'$ selbst durch ϑ teilbar ist, so muss sich der zweite Teil $A''B'$ ebenfalls durch ϑ teilen lassen.

Die Zahl A'' ist als Rest der Division durch A' kleiner als A', und ferner kann sie nicht gleich 0 sein. Denn wäre dies der Fall, so würde ϑ durch A' teilbar, also keine Primzahl sein. Aus der Annahme, dafs das Produkt $A'B'$ durch ϑ teilbar sei, folgt somit, dafs ein anderes Produkt, welches kleiner ist als $A'B'$, ohne gleich Null zu sein, ebenfalls durch ϑ teilbar ist.

Mittelst derselben Schlussfolgerung leitet man aus dem Produkte $A''B'$ ein anderes Produkt $A'''B'$ oder $A''B''$ ab, welches noch kleiner ist, und welches teilbar durch ϑ, aber nicht gleich Null ist.

Indem man die Reihe dieser abnehmenden Produkte weiter fortsetzt, gelangt man notwendigerweise zu einer Zahl, welche kleiner ist als ϑ. Eine Zahl aber, welche kleiner als ϑ und von Null verschieden ist, kann unmöglich teilbar sein durch ϑ. Mithin kann die Annahme, von der wir ausgegangen waren, nicht richtig sein.

Wenn sich also von beiden Zahlen A und B keine durch ϑ teilen läfst, so kann auch ihr Produkt AB nicht durch ϑ teilbar sein.

VII.

Auf dem soeben bewiesenen Satze beruht vollständig die Lehre von den **inkommensurablen** Gröfsen. Denn gäbe es z. B.

einen rationalen Bruch $\frac{m}{n}$, welcher gleich $\sqrt{2}$ wäre, so müſste $\frac{m^2}{n^2} = 2$ sein. Es müsste demnach m^2 durch jede der Primzahlen, welche n teilen, ebenfalls sich teilen lassen. Wenn aber der Bruch $\frac{m}{n}$ als irreduktibel vorausgesetzt wird, so hat m keinen Teiler mit n gemeinschaftlich; mithin kann dem vorhergehenden Satze zufolge auch m^2 mit n keinen Teiler gemeinsam haben. Es ist daher unmöglich, daſs $\frac{m^2}{n^2} = 2$ sei.

Ueberhaupt kann eine beliebige Potenz der Zahl a keine andern Primzahlen zu Teilern haben als a selbst. Wenn es daher keine ganze Zahl x von der Beschaffenheit giebt, daſs $x^n = b$ ist, wo b eine gegebene ganze Zahl bedeutet, so kann es auch keinen Bruch $\frac{x}{y}$ geben, so daſs $\frac{x^n}{y^n} = b$ wäre.

VIII.

Jede beliebige **Zahl** N kann, wenn sie **nicht Primzahl** ist, **durch das Produkt** von **mehreren Primzahlen** $\alpha, \beta, \gamma, \ldots$, jede derselben auf irgend eine Potenz erhoben, **dargestellt werden**, so daſs man immer setzen kann: $N = \alpha^m \beta^n \gamma^p \cdots$.

Das **Verfahren**, diese Zerlegung auszuführen, besteht darin, daſs man versucht, die Zahl N durch jede der Primzahlen 2, 3, 5, 7, 11, ... zu dividieren, wobei man mit den kleinsten anfängt. Geht die Division durch eine dieser Zahlen α auf, so wiederholt man sie so oft als möglich, z. B. m-mal, und erhält dadurch, indem man den letzten Quotienten mit P bezeichnet, $N = \alpha^m P$.

Läſst sich die Zahl P nicht mehr durch α teilen, so braucht man nicht erst mehr die Division von P durch eine Primzahl, welche kleiner ist als α, zu versuchen. Denn wenn P durch $\vartheta < \alpha$ teilbar wäre, so würde offenbar auch N durch ϑ teilbar sein, was unserer Annahme zuwiderläuft. Man wird daher P nur durch Primzahlen zu dividieren brauchen, welche gröſser sind als α. Auf diese Weise wird man nach und nach $P = \beta^n Q$, $Q = \gamma^n R$, u. s. w. finden, und dies giebt $N = \alpha^m \beta^n \gamma^p \ldots$

IX.

Hat man die Division einer gegebenen Zahl N durch die Primzahlen, welche **kleiner als** $\sqrt{N}$ sind, versucht, und

findet man unter diesen keine, welche in N aufgehen, so folgt daraus mit Sicherheit, dafs N eine Primzahl ist.

Denn nimmt man an, dafs N durch eine Primzahl $\vartheta > \sqrt{N}$ teilbar sei, so würde man, wenn man den Quotienten mit P bezeichnet, $N = \vartheta P$ erhalten. Da aber $\vartheta > \sqrt{N}$ ist, so würde

$$P = \frac{N}{\vartheta} < \frac{N}{\sqrt{N}} < \sqrt{N}$$

sein; mithin würde N durch eine Zahl P, welche kleiner ist als $\sqrt{N}$, und somit umsomehr durch eine Primzahl, welche kleiner als $\sqrt{N}$ ist, teilbar sein. Dies ist aber gegen unsere Annahme.

Auf diese Weise kann man also finden, ob eine gegebene Zahl N **Primzahl ist oder nicht.** Dieses Verfahren ist indessen, obwohl es, wie wir später zeigen werden, einige Abkürzungen zulässt, im Allgemeinen recht weitläufig und beschwerlich. Deshalb haben mehrere Mathematiker es für nützlich gehalten, **Primzahltafeln** von grösserer oder geringerer Ausdehnung zu konstruieren.

Die einfachste Art, solche Tafeln herzustellen, besteht darin, dafs man zunächst der Reihe nach alle ungeraden Zahlen 1, 3, 5, 7, ... bis zu 100 000 etwa oder bis zu einer beliebigen andern Grenze hinschreibt. Ist diese Reihe gebildet, so streicht man nach und nach alle Vielfachen von 3, ferner alle Vielfachen von 5, 7, u. s. w. weg, indem man nur die ersten Glieder 3, 5, 7, u. s. w. beibehält, welche durch die vorhergehenden Operationen nicht weggefallen sind. Auf diese Weise sieht man, dafs alle übrigbleibenden Zahlen nur durch sich selbst teilbar und in Folge dessen Primzahlen sind. Am Ende dieses Werkes wird man eine Tafel No. IX finden, welche die Primzahlen bis zu 1229 enthält. In einem Werke, das den Titel führt: Georgii Vega Tabulae logarithmico-trigonometricae, Lipsiae 1797, findet man eine Tafel, die sich bis zu 400 000 erstreckt, und die überdies den Vorteil gewährt, dafs sie für jede unterhalb dieser Grenze liegende zusammengesetzte Zahl die kleinste Primzahl, welche ein Teiler derselben ist, angiebt. Indessen hegten die Mathematiker schon lange den Wunsch, dafs die Tafel der Primzahlen mindestens bis zu einer Million fortgesetzt würde. Herr Chernac, Professor zu Deventer, entsprach zuerst diesem Wunsche, indem er sein Cribrum arithmeticum, in dem man die Primzahlen und die Teiler der andern Zahlen bis zu einer Million findet, veröffentlichte. Bald darauf gab Herr Burckhardt, der Mittel zur erheblichen Vereinfachung der Konstruktion solcher Tafeln gefunden hatte, eine Tafel heraus, welche in

einem nicht zu starken Bande die Primzahlen von 1 bis 3036000 und die kleinsten Teiler der andern Zahlen enthält. Diejenigen, welche sich mit der unbestimmten Analysis beschäftigen, haben also die Wahl zwischen zwei Tabellenwerken, die ihnen gleicherweise nützlich sein können, das eine wegen seiner leichteren Handhabung, das andere wegen seiner grösseren Ausdehnung.

X.

Ist eine Zahl N auf die Form $\alpha^m \beta^n \gamma^p \ldots$ gebracht, so wird auch jeder Teiler dieser Zahl von der Form $\alpha^\mu \beta^\nu \gamma^\pi \ldots$ sein, wo die Exponenten $\mu, \nu, \pi, \ldots$ die Zahlen $m, n, p, \ldots$ nicht übersteigen können. Es folgt hieraus, dafs die Teiler der Zahl N sämtlich durch die verschiedenen Glieder der Entwicklung des Produkts:

$$P = (1 + \alpha + \alpha^2 + \cdots + \alpha^m)(1 + \beta + \beta^2 + \cdots + \beta^n) \cdots$$

gegeben werden. Mithin ist die **Anzahl** aller dieser Teiler gleich:

$$(m + 1)(n + 1)(p + 1) \ldots,$$

und zugleich ist die **Summe** eben dieser Faktoren gleich P, und dieses läfst sich auf die Form bringen:

$$P = \frac{\alpha^{m+1} - 1}{\alpha - 1} \cdot \frac{\beta^{n+1} - 1}{\beta - 1} \cdot \frac{\gamma^{p+1} - 1}{\gamma - 1} \cdots.$$

So ist z. B., da $360 = 2^3 \cdot 3^2 \cdot 5^1$ ist, die Anzahl der Teiler von 360 gleich:

$$4 \,.\, 3 \,.\, 2 = 24$$

und die Summe derselben gleich:

$$\frac{2^4 - 1}{2 - 1} \cdot \frac{3^3 - 1}{3 - 1} \cdot \frac{5^2 - 1}{5 - 1} = 15 \cdot 13 \cdot 6 = 1170.$$

XI.

Man kann leicht eine Zahl finden, welche soviel Teiler hat als man will. Sucht man z. B. eine Zahl, welche 36 Teiler hat, so zerlege man 36 in Faktoren, die Primzahlen sein können oder nicht, z. B. in 4 . 3 . 3, und vermindere jeden dieser Faktoren um eine Einheit. Dies giebt 3 . 2 . 2. Mithin ist $\alpha^3\beta^2\gamma^2$ eine der Formen der gesuchten Zahl, wenn α, β, γ von einander verschiedene Primzahlen bedeuten. Die Faktoren 6, 3, 2 würden eine andere Form $\alpha^5\beta^2\gamma^1$ ergeben, bei welcher die einfachste der in ihr enthaltenen Zahlen $2^5 \,.\, 3^2 \,.\, 5 = 1440$ ist.

XII.

Wenn man sucht, auf wieviel Arten die Zahl $N = \alpha^m \beta^n \gamma^p \ldots$ das Produkt von **zwei** Faktoren A und B sein könne, so findet man diese Anzahl gleich:

$$\frac{1}{2}(m+1)(n+1)(p+1)\ldots.$$

Denn neben jedem Teiler A kommt der zu ihm inverse $\frac{N}{A}$ oder B vor; mithin ist die Anzahl der Gröfsen AB oder BA die Hälfte von der Anzahl der Teiler von N.

Wäre die Zahl N ein Quadrat, so würden alle Exponenten m, n, p.. gerade Zahlen sein, und es würde somit die Hälfte des Produkts $(m+1)(n+1)(p+1)\ldots$ den Bruch $\frac{1}{2}$ enthalten. Für diesen müsste man die Einheit nehmen.

XIII.

Sollen die beiden Faktoren, in welche man die Zahl N zerlegt, **prim** zu einander sein, so ist die Anzahl der möglichen Combinationen nicht mehr von den Exponenten $m, n, p, \ldots$ abhängig, sondern sie ist dieselbe, als ob die Zahl N nur einfach gleich $\alpha\beta\gamma\delta\ldots$ wäre, so dafs man, wenn k die Anzahl der ungleichen Primfaktoren bezeichnet, für die Zahl, welche angiebt, wie oft sich N in zwei zu einander prime Faktoren zerlegen lässt, die Zahl 2^{k-1} erhält.

So lässt sich z. B. die Zahl 1800 zwar auf 18 verschiedene Arten in zwei Faktoren zerlegen, aber nur auf 4 verschiedene Arten in zwei Faktoren, die prim zu einander sind; denn es ist $1800 = 2^3 . 3^2 . 5^2$ und $2^{3-1} = 4$.

XIV.

Es sei die Aufgabe gestellt, für eine gegebene Zahl N zu untersuchen, wieviel Zahlen es giebt, die **prim** zu N und zugleich **kleiner** als N sind.

Um diese Aufgabe zu lösen, werden wir nach und nach den Einfluss zu ermitteln suchen, welchen die verschiedenen Primfaktoren auf das Resultat ausüben.

Es sei zuerst $N = \alpha M$, wo α eine Primzahl und M einen beliebigen Faktor bedeutet, der noch durch α oder eine Potenz von α teilbar sein könnte. Wenn man die Reihe der natürlichen Zahlen $1, 2, 3 \ldots N$ betrachtet, so bilden diejenigen Glieder dieser Reihe,

welche durch α teilbar sind, ihrerseits wieder eine Reihe α, 2α, $3\alpha, \ldots M\alpha$. Die Anzahl dieser Glieder ist M. Nennt man also x die Anzahl der Glieder der ersten Reihe, welche nicht teilbar sind durch α, so hat man:

$$x = M\alpha - M = M(\alpha - 1).$$

Ist zweitens $N = \alpha\beta M$, wo α und β zwei verschiedene Primzahlen und M ein beliebiger Faktor ist, so kann man in der Reihe $1, 2, 3 \ldots N$ drei Arten von Gliedern unterscheiden:

1) die x Glieder, welche weder durch α noch durch β teilbar sind;

2) die Glieder, welche durch die eine dieser Primzahlen, aber nicht durch beide zugleich teilbar sind;

3) die durch $\alpha\beta$ teilbaren Glieder.

Die Anzahl der durch α teilbaren Glieder ist $\frac{N}{\alpha}$ oder $M\beta$. Schliefst man aber davon noch die durch β teilbaren Glieder aus, so reduciert sich diese Anzahl, nach dem, was wir vorher schon gefunden haben, auf $M(\beta - 1)$. Ebenso ist die Anzahl der allein durch β (nicht durch α) teilbaren Glieder gleich $M(\alpha - 1)$. Endlich ist die Anzahl der durch $\alpha\beta$ teilbaren Glieder gleich M. Man erhält also

$$\alpha\beta M = x + M(\beta - 1) + M$$
$$+ M(\alpha - 1),$$

und hieraus folgt:

$$x = M(\alpha - 1)(\beta - 1) = N\left(1 - \frac{1}{\alpha}\right)\left(1 - \frac{1}{\beta}\right).$$

Ist drittens $N = \alpha\beta\gamma M$, so können wir in ähnlicher Weise wie vorher in der Reihe $1, 2, 3, \ldots N$ vier Arten von Gliedern unterscheiden:

1) die x Glieder, welche durch keinen der Faktoren α, β, γ teilbar sind;

2) die Glieder, welche nur durch einen dieser Faktoren teilbar sind;

3) die Glieder, welche sich nur durch zwei derselben teilen lassen,

4) die Glieder, welche durch alle drei teilbar sind.

Durch α teilbare Glieder sind überhaupt $\frac{N}{\alpha}$ oder $M\beta\gamma$ vorhanden; betrachtet man aber unter ihnen nur die, welche prim zu β und γ sind, so reduciert sich ihre Anzahl, wie wir beim zweiten Falle gefunden haben, auf $M(\beta - 1)(\gamma - 1)$.

Durch $\alpha\beta$ teilbare Glieder giebt es im Ganzen $\frac{N}{\alpha\beta}$ oder $M\gamma$;

betrachtet man aber von diesen nur die zu γ primen Glieder, so reduciert sich ihre Anzahl auf $M(\gamma - 1)$.

Endlich kommen $\frac{N}{\alpha\beta\gamma}$ oder M durch $\alpha\beta\gamma$ teilbare Glieder vor.

Demnach erhält man:

$$\begin{aligned}\alpha\beta\gamma M = x &+ M(\beta - 1)(\gamma - 1) + M(\gamma - 1) + M \\ &+ M(\gamma - 1)(\alpha - 1) + M(\alpha - 1) \\ &+ M(\alpha - 1)(\beta - 1) + M(\beta - 1).\end{aligned}$$

Setzt man für den Augenblick:

$$\alpha - 1 = \alpha', \quad \beta - 1 = \beta', \quad \gamma - 1 = \gamma',$$

so wird die linke Seite gleich $M(\alpha' + 1)(\beta' + 1)(\gamma' + 1)$ oder gleich:

$$\begin{aligned}M\alpha'\beta'\gamma' &+ M\beta'\gamma' + M\gamma' + M \\ &+ M\gamma'\alpha' + M\alpha' \\ &+ M\alpha'\beta' + M\beta',\end{aligned}$$

und die rechte Seite unterscheidet sich von dieser Gröfse nur durch das erste Glied, welches in ihr x anstatt $M\alpha'\beta'\gamma'$ ist. Es ist demnach:

$$x = M\alpha'\beta'\gamma',$$

oder:

$$x = N\left(1 - \frac{1}{\alpha}\right)\left(1 - \frac{1}{\beta}\right)\left(1 - \frac{1}{\gamma}\right).$$

Dieselbe Schlussweise wendet man leicht auf eine gröfsere Anzahl von Faktoren an, und man sieht, dafs das Resultat stets von derselben Form sein wird.

XV.

Da jede Zahl N auf die Form $\alpha^m\beta^n\gamma^p\ldots$ gebracht werden kann, welche in dem allgemeinen Ausdrucke $M\alpha\beta\gamma\ldots$ enthalten ist, so ist hiernach klar, dafs man aus der Formel

$$x = N\left(1 - \frac{1}{\alpha}\right)\left(1 - \frac{1}{\beta}\right)\left(1 - \frac{1}{\gamma}\right)\cdots$$

erkennt, wie viele Zahlen es giebt, die prim zu N und zugleich kleiner als N sind.

So ist z. B.

$$60 = 2^2 . 3 . 5 \text{ und } 60\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 16.$$

Es giebt daher 16 Zahlen, die relativ prim zu 60 und kleiner als 60 sind. Diese Zahlen sind:

1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59.

XVI.

Wir wollen jetzt untersuchen, wievielmal eine gegebene Primzahl ϑ in der Reihe der natürlichen Zahlen von 1 bis N als Faktor vorkommt, oder, was dasselbe ist, welches die höchste Potenz von ϑ ist, welche in dem Produkte $1 \,.\, 2 \,.\, 3 \ldots N$ aufgeht.

Zu dem Zwecke bezeichnen wir durch $E\left(\frac{n}{a}\right)$ die gröfste ganze Zahl, welche in dem Bruche $\frac{n}{a}$ enthalten ist, und nennen die gesuchte Zahl oder den Exponenten von ϑ x. Dann erhalten wir:

$$x = E\left(\frac{N}{\vartheta}\right) + E\left(\frac{N}{\vartheta^2}\right) + E\left(\frac{N}{\vartheta^3}\right) + \cdots,$$

wo diese Reihe so lange fortzusetzen ist, als der Zähler gröfser ist als der Nenner.

Offenbar stellt nämlich $E\left(\frac{N}{\vartheta}\right)$ die Anzahl der Glieder der Reihe $1, 2, 3, \ldots N$ dar, welche teilbar sind durch ϑ; ebenso stellt $E\left(\frac{N}{\vartheta^2}\right)$ die Anzahl der Glieder derselben Reihe dar, welche teilbar sind durch ϑ^2, und so fort. Wenn es nun in dem Produkte $1 \,.\, 2 \,.\, 3 \ldots N$ keine durch ϑ^2 teilbaren Glieder gäbe, so würde die Anzahl der Faktoren ϑ, welche dieses Produkt teilen, einfach $E\left(\frac{N}{\vartheta}\right)$ sein. Kommen aber überdies solche durch ϑ^2 teilbaren Glieder vor, so wird durch jedes dieser Glieder ein neuer Faktor ϑ zu demjenigen hinzutreten, welcher bereits in $E\left(\frac{N}{\vartheta}\right)$ aufgenommen war, so dafs, wenn man nur die durch ϑ und die durch ϑ^2 teilbaren Glieder berücksichtigt, die Anzahl der Faktoren ϑ gleich $E\left(\frac{N}{\vartheta}\right) + E\left(\frac{N}{\vartheta^2}\right)$ wird. In derselben Weise kommt durch jedes durch ϑ^3 teilbare Glied ein weiterer Faktor ϑ zu den bereits gezählten hinzu, so dafs die Gesamtzahl der Faktoren ϑ gleich $E\left(\frac{N}{\vartheta}\right) + E\left(\frac{N}{\vartheta^2}\right) + E\left(\frac{N}{\vartheta^3}\right)$ wird. So geht es weiter, bis man zu einer Potenz $\vartheta^i > N$ gelangt; alsdann bricht die Reihe der E ab, da $\frac{N}{\vartheta^i}$ kleiner als 1 und somit die darin enthaltene Zahl $E\left(\frac{N}{\vartheta^i}\right) = 0$ ist.

XVII.

Soll z. B. gefunden werden, wie oft der Faktor 7 in dem Produkt der natürlichen Zahlen von 1 bis 10 000 enthalten ist, so stellen wir folgende kurze Rechnung an:

$$E\left(\frac{10000}{7}\right) = 1428$$

$$E\left(\frac{10000}{7^2}\right) = E\left(\frac{1428}{7}\right) = 204$$

$$E\left(\frac{10000}{7^3}\right) = E\left(\frac{204}{7}\right) = 29$$

$$E\left(\frac{10000}{7^4}\right) = E\left(\frac{29}{7}\right) = 4$$

$$E\left(\frac{10000}{7^5}\right) = E\left(\frac{4}{7}\right) = 0.$$

Die Summe aller dieser Zahlen ist gleich 1665; mithin ist das in Rede stehende Produkt teilbar durch 7^{1665}.

Wenn die gegebene Zahl N eine ganze Potenz von 7 gewesen wäre, so würde man genau $x = N\left(\frac{1}{7} + \frac{1}{7^2} + \cdots\right) = \frac{N-1}{6}$ gehabt haben. Ist allgemein $N = \vartheta^m$, so ist die Anzahl der Faktoren ϑ, welche in dem Produkte $1 \,.\, 2 \,.\, 3 \ldots N$ enthalten sind, gleich:

$$x = \frac{N-1}{\vartheta - 1}.$$

Setzt man, welche Annahme jederzeit möglich ist,

$$N = A\vartheta^m + B\vartheta^n + C\vartheta^p + \cdots,$$

wo die Koefficienten $A, B, C \ldots$ kleiner sind als ϑ, so folgt daraus:

$$x = \frac{N - A - B - C - \cdots}{\vartheta - 1}.$$

XVIII.

In dem besonderen Falle, wo $\vartheta = 2$, ergiebt sich, falls $N = 2^m$ ist,

$$x = N - 1,$$

und setzt man allgemein:

$$N = 2^m + 2^n + 2^p + \cdots,$$

so erhält man:

$$x = N - k,$$

wo k die Anzahl der Glieder $2^m, 2^n, 2^p, \ldots,$ aus denen der Wert von N besteht, bedeutet.

Will man z. B. wissen, wie oft die Zahl 2 als Faktor in der Reihe der natürlichen Zahlen von 1 bis 1000 vorkommt, so zerlege man 1000 in Potenzen von 2, nämlich

$$2^9 + 2^8 + 2^7 + 2^6 + 2^5 + 2^3.$$

Da die Anzahl dieser Glieder 6 ist, so ist die gesuchte Zahl $1000 - 6$ oder 994.

Dasselbe Resultat erhält man nicht minder leicht aus der allgemeinen Formel; denn es ist:

$$E\left(\frac{1000}{2}\right) = 500$$
$$E\left(\frac{500}{2}\right) = 250$$
$$E\left(\frac{250}{2}\right) = 125$$
$$E\left(\frac{125}{2}\right) = 62$$
$$E\left(\frac{62}{2}\right) = 31$$
$$E\left(\frac{31}{2}\right) = 15$$
$$E\left(\frac{15}{2}\right) = 7$$
$$E\left(\frac{7}{2}\right) = 3$$
$$E\left(\frac{3}{2}\right) = 1,$$

und die Summe aller dieser Zahlen ist gleich 994.

XIX.

Jede Primzahl, mit Ausnahme von 2 und 3, ist in der Formel $6x \pm 1$ enthalten.

Denn dividiert man eine ungerade Zahl durch 6, so kann der Rest nur eine der Zahlen 1, 3, 5 sein. Mithin kann jede ungerade Zahl durch eine der Formeln $6x + 1$, $6x + 3$, $6x + 5$ dargestellt werden. Die zweite kann keine Primzahlen enthalten, da sie durch 3 teilbar und die 3 selbst ausgenommen ist. Ferner enthält die Formel $6x + 5$ dieselben Zahlen wie $6x - 1$. Mithin ist jede Primzahl, ausser 2 und 3, in der Formel $6x \pm 1$ enthalten.

Umgekehrt folgt hieraus **nicht**, dafs auch jede in der Formel $6x \pm 1$ enthaltene Zahl eine Primzahl sein müfste. Man würde finden, dafs dies nicht der Fall ist für $x = 4, 6, \ldots$

XX.

Überhaupt giebt es **keine algebraische** Formel, welche die Eigenschaft besäſse, **lauter** Primzahlen darzustellen. Denn nimmt man z. B. die Formel:

$$P = ax^3 + bx^2 + cx + d$$

und setzt voraus, daſs der Wert von P für $x = k$ gleich der Primzahl p sei, so erhält man, wenn man $x = k + py$ setzt, wo y eine beliebige ganze Zahl bedeutet:

$$P = p + (3ak^2 + 2bk + c)py + (3ak + b)p^2y^2 + ap^3y^3.$$

Hieraus ersieht man, daſs P keine Primzahl sein kann, da sie teilbar durch p und von p verschieden ist.

Nichtsdestoweniger giebt es einige Formeln, die wegen der Menge der in ihnen enthaltenen Primzahlen bemerkenswert sind. Eine solche Formel ist:

$$x^2 + x + 41,$$

welche Euler in den Abhandlungen der Berliner Akademie vom Jahre 1772 Seite 36 erwähnt. Setzt man in dieser nach einander $x = 0, 1, 2, 3, \ldots,$ so erhält man die Reihe 41, 43, 47, 53, 61, 71, …, deren vierzig erste Glieder Primzahlen sind.

Hierzu kann man auch die Formel

$$x^2 + x + 17$$

rechnen, in welcher die ersten sechszehn Glieder Primzahlen sind; ferner die Formel

$$2x^2 + 29,$$

deren erste neunundzwanzig Glieder Primzahlen sind, und noch viele andere.

XXI.

Wenn man schon keine algebraische Formel finden kann, welche einzig und allein Primzahlen enthielte, so läſst sich noch viel weniger eine solche finden, welche absolut **alle** diese Zahlen enthielte und der Ausdruck ihres **allgemeinen** Gesetzes wäre. Dieses Gesetz dürfte sehr schwer zu finden sein, und es ist kaum zu hoffen, daſs man jemals dazu gelangen werde. Doch hindert dies nicht, dass man für die Primzahlen eine groſse Anzahl von **allgemeinen Eigenschaften,** welche helles Licht über ihre Natur verbreiten, zu entdecken und zu beweisen imstande ist.

Zunächst kann man in aller Strenge beweisen, daſs die **Anzahl** der Primzahlen **unendlich groſs** ist.

Denn wenn die Reihe der Primzahlen 1, 2, 3, 5, 7, 11 ... endlich und p die letzte oder gröſste von allen diesen Zahlen wäre, so müſste eine beliebige Zahl N stets durch irgend eine der Primzahlen 1, 2, 3, 5 ... p teilbar sein. Stellt man aber durch P das Produkt aller dieser Zahlen*) dar, so wird offenbar, wenn man $P + 1$ durch irgend eine der Primzahlen bis p dividiert, der Rest 1 übrigbleiben. Mithin kann die Annahme, daſs p die gröſste der Primzahlen sei, nicht richtig sein, und es ist somit die Anzahl der Primzahlen unendlich groſs.

Diesen Satz kann man noch auf eine direkte und sehr elegante Weise beweisen, indem man zeigt, daſs die Reihe der reciproken Werte der Primzahlen $\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \cdots$ eine unendlich groſse Summe besitzt. (Euler. Introd. in Anal. infin. Seite 235.)

XXII.

Alle ungeraden Zahlen lassen sich durch die Formel $2x + 1$ darstellen, und diese enthält, je nachdem x gerade oder ungerade ist, die beiden Formen $4x + 1$ und $4x - 1$ oder $4x + 3$. Hieraus entspringen zwei **Hauptklassen** der Primzahlen; die eine enthält alle Primzahlen von der Form $4x + 1$, nämlich:

1, 5, 13, 17, 29, 37, 41, 53, 61, 73, ...

die andere alle Primzahlen von der Form $4x - 1$ oder $4x + 3$, nämlich:

3, 7, 11, 19, 23, 31, 43, 47, 59, ...

---

*) Nimmt man in dem Produkte P nach einander zwei, drei, vier u. s. w. Faktoren, so ergeben sich für die Zahl $P + 1$ die Werte 3, 7, 31, 211, 2311, 30031, ... Die fünf ersten Glieder dieser Reihe sind Primzahlen, und dies könnte zu der Vermutung verleiten, daſs es auch die folgenden sein werden. Indessen erweist sich diese Vermutung bald als unrichtig, wenn man das sechste Glied 30031 untersucht, das sich als das Produkt von 59 und 509 darstellt. Überhaupt ist es eine schwierige und bisher nicht gelöste Aufgabe, eine Primzahl zu finden, welche gröſser als eine gegebene Zahl ist. Fermat hatte (ohne anzugeben, daſs er einen Beweis dafür habe) behauptet, daſs die Formel $2^x + 1$ stets Primzahlen gebe, wenn man für x ein Glied der geometrischen Progression 1, 2, 4, 8, 16, ... nehme. Diese Formel, welche eine sehr einfache Lösung der eben erwähnten Aufgabe geliefert hätte, hat sich aber als unrichtig herausgestellt. Denn, wie Euler bemerkt hat, erhält man, wenn man $x = 32$ setzt, $2^x + 1 = 641 \cdot 6700417$. Anm. d. Verf.



Die allgemeine Form $4x + 1$ teilt sich wieder in zwei andere Formen $8x + 1$ und $8x - 3$ oder $8x + 5$; ebenso teilt sich die Form $4x + 3$ wieder in zwei andere Formen $8x + 3$ und $8x + 7$ oder $8x - 1$. Mithin zerfallen die Primzahlen, bezüglich der Vielfachen von 8, in folgende vier Hauptformen:

$8x + 1$: 1, 17, 41, 73, 89, 97, 113, 137, ...

$8x + 3$: 3, 11, 19, 43, 59, 67, 83, 107, ...

$8x + 5$: 5, 13, 29, 37, 53, 61, 101, 109, ...

$8x + 7$: 7, 23, 31, 47, 71, 79, 103, 127, ...

Dieselben geben Anlafs zu verschiedenen Sätzen, welche diese Formen charakterisieren, und die wir in der Folge entwickeln werden.

XXIII.

Wir haben bereits gesehen, dafs die Primzahlen, betrachtet in Bezug auf die Vielfachen von 6, von einer der Formen $6x + 1$ und $6x - 1$ oder $6x + 5$ sind. In diesen Formen kann x gerade oder ungerade sein. Daraus ergeben sich, in Bezug auf die Vielfachen von 12, die vier Formen:

$$12x + 1, \ 12x + 5, \ 12x + 7, \ 12x + 11,$$

deren jede unendlich viele Primzahlen enthält.

Ist a eine beliebig gegebene Zahl, so kann allgemein jede ungerade Zahl ausgedrückt werden durch die Formel $4ax \pm b$, in welcher b eine ungerade Zahl und kleiner als $2a$ ist, oder, was auf dasselbe hinauskommt, durch die Formel $4ax + b$, in welcher b eine ungerade Zahl, positiv und kleiner als $4a$ ist. Wenn man von allen möglichen Werten von b diejenigen ausnimmt, welche einen gemeinsamen Teiler mit a haben, so werden die übrig bleibenden Formen $4ax + b$ alle Primzahlen (mit Ausnahme derjenigen, welche in $4a$ aufgehen) enthalten und diese werden, mit Bezug auf die Vielfachen von $4a$, in soviel Klassen oder Formen zerfallen, als es verschiedene Werte von b giebt. Die **Anzahl dieser Formen** ist offenbar dieselbe wie diejenige der Zahlen, welche kleiner als $4a$ und prim zu $4a$ sind. Ist daher $4a = 2^m \alpha^n \beta^p \ldots$, wo $\alpha, \beta, \ldots$ Primzahlen bedeuten, so wird die Anzahl dieser Formen durch die Formel gegeben:

$$\mathfrak{a} = 4a\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{\alpha}\right)\left(1 - \frac{1}{\beta}\right)\cdots$$



XXIV.

Ist z. B. $4a = 60$, so ergiebt sich $a = 16$. Folglich zerfallen, in Bezug auf die Vielfachen von 60, sämtliche Primzahlen (2, 3, 5, die Teiler von 60, ausgenommen) in sechzehn Formen, nämlich:

$$60x + 1,\ 60x + 7,\ 60x + 11,\ 60x + 13,$$
$$60x + 17,\ 60x + 19,\ 60x + 23,\ 60x + 29,$$
$$60x + 31,\ 60x + 37,\ 60x + 41,\ 60x + 43,$$
$$60x + 47,\ 60x + 49,\ 60x + 53,\ 60x + 59.$$

Wir werden überdies später beweisen, daſs die Verteilung der Primzahlen auf diese sechzehn Formen eine gleichmäſsige ist, oder nach Verhältnissen erfolgt, die sich mehr und mehr der Gleichheit nähern.

Erster Hauptteil.

Entwicklung von verschiedenen Methoden und Sätzen, welche sich auf die unbestimmte Analysis beziehen.

§ 1.

Von den Kettenbrüchen.

1.

Das Verfahren, um eine beliebige rationale oder irrationale Gröfse x in einen Kettenbruch zu verwandeln, beruht darauf, dafs man nach und nach die Ausdrücke bildet:

$$x = \alpha + \frac{1}{x'}, \quad x' = \alpha' + \frac{1}{x''}, \quad x'' = \alpha'' + \frac{1}{x'''}, \cdots,$$

wo α die gröfste in x enthaltene ganze Zahl, α' die gröfste in x' enthaltene ganze Zahl u. s. w. bedeutet. Auf diese Weise wird offenbar die Gröfse x in den folgenden Kettenbruch

$$\alpha + \frac{1}{\alpha' + \frac{1}{\alpha'' + \frac{1}{\alpha''' + \cdots}}}$$

verwandelt, und dieser wird eine endliche oder unendliche Anzahl von Gliedern enthalten, je nachdem die Gröfse x rational oder irrational ist.

Diese Glieder oder Quotienten α, α', α'', ... werden immer, ebenso wie die Gröfse x, **positiv** vorausgesetzt (wäre x kleiner als 1, so würde der erste α gleich 0 sein). Zuweilen ist es indessen, um die Reihe convergenter zu machen, zweckmäfsig, auch negative Quotienten zuzulassen; jedoch ist dies eine Ausnahme, die jedesmal ausdrücklich angegeben werden mufs, und von der wir im folgenden nirgends Gebrauch machen werden.

2.

Wenn die Gröfse x ein rationaler Bruch $\frac{M}{N}$ ist, so hat man nur, um diese Gröfse in einen Kettenbruch zu verwandeln, mit den

beiden Zahlen M und N ebenso zu verfahren, als ob man den gröfsten gemeinsamen Teiler derselben suchte.

Nimmt man $M > N$ an, so ist das Schema für diese Rechnung:

$$\text{Rest}\ \frac{M}{P}\left\{\frac{N}{\alpha}\right., \quad \text{Rest}\ \frac{N}{Q}\left\{\frac{P}{\alpha'}\right., \quad \text{Rest}\ \frac{P}{R}\left\{\frac{Q}{\alpha''}\right., \ \text{u. s. w.}$$

Hiernach erhält man der Reihe nach:

$$\frac{M}{N} = \alpha + \frac{P}{N},$$
$$\frac{N}{P} = \alpha' + \frac{Q}{P},$$
$$\frac{P}{Q} = \alpha'' + \frac{R}{Q},$$
$$\text{u. s. w.}$$

Mithin:

$$\frac{M}{N} = \alpha + \frac{1}{\alpha' + \frac{1}{\alpha'' + \ldots}}, \quad \frac{N}{M} = \frac{1}{\alpha + \frac{1}{\alpha' + \frac{1}{\alpha'' + \ldots}}}$$

In diesem Falle sind die Glieder des Kettenbruchs nichts anderes als die bei der Berechnung des gemeinschaftlichen Teilers der Reihe nach gefundenen Quotienten, und es ist klar, dafs der Kettenbruch stets auf eine **bestimmte** Anzahl von Gliedern **beschränkt** ist, die mehr oder weniger grofs sein kann, je nachdem der Bruch $\frac{M}{N}$ mehr oder weniger zusammengesetzt ist.

3.

Die aufeinanderfolgenden Glieder $\alpha, \alpha', \alpha'', \ldots$ des Kettenbruchs haben wir **Quotienten** genannt. In ähnlicher Weise werden wir die Gröfsen $x, x', x'', \ldots$, welche sich aus der Berechnung der Entwicklung ergeben und deren Hauptbestandteile die ganzen Zahlen $\alpha, \alpha', \alpha'', \ldots$ bilden, **vollständige Quotienten** nennen. Jeder vollständige Quotient enthält aufser der in ihm vorkommenden ganzen Zahl sämtliche nachfolgenden Quotienten des Kettenbruches implicite in sich, da man ja erst durch die Entwicklung dieses vollständigen Quotienten nach und nach alle folgenden Quotienten findet.

Wenn man einen algebraischen Ausdruck hat, welcher den Wert des bis zum Gliede $\alpha^{(n)}$ einschliesslich fortgesetzten Kettenbruches darstellt, und wenn man in diesen Ausdruck an Stelle von $\alpha^{(n)}$ den vollständigen Quotienten $x^{(n)}$ einsetzt, so wird das Resultat offenbar der genaue Wert von x sein. Denn selbst wenn der Kettenbruch sich ins Unendliche erstreckte, würde man in aller Strenge

$$x = \alpha + \frac{1}{x'}, \quad x = \alpha + \frac{1}{\alpha' + \frac{1}{x''}}, \quad x = \alpha + \frac{1}{\alpha' + \frac{1}{\alpha'' + \frac{1}{x'''}}}, \text{ u. s. w.}$$

haben. Daraus folgt, dafs man mit Hülfe eines jeden vollständigen Quotienten stets den vollständigen und genauen Wert der entwickelten Gröfse wieder hervorbringen kann, wie weit man auch die Entwicklung fortgesetzt haben möge. Diese Eigenschaft wird in der Folge eine grofse Anzahl nützlicher Anwendungen finden.

4.

Ist der Kettenbruch

$$x = \alpha + \frac{1}{\beta + \frac{1}{\gamma + \frac{1}{\delta + \cdots}}}$$

gegeben, so mufs man, wenn man ihn in einen gewöhnlichen Bruch verwandeln oder seinen Wert, welches auch die Anzahl seiner Glieder sein möge, finden will, auf das Gesetz achten, welches die erhaltenen Resultate befolgen, wenn man nach und nach das erste Glied, die beiden ersten Glieder, die drei ersten Glieder u. s. w. dieser Gröfse nimmt. Nun erhält man durch die gewöhnlichen Reduktionen:

$$\alpha = \frac{\alpha}{1}$$

$$\alpha + \frac{1}{\beta} = \frac{\alpha\beta + 1}{\beta}$$

$$\alpha + \frac{1}{\beta + \frac{1}{\gamma}} = \frac{\alpha\beta\gamma + \gamma + \alpha}{\beta\gamma + 1}$$

$$\alpha + \frac{1}{\beta + \frac{1}{\gamma + \frac{1}{\delta}}} = \frac{\alpha\beta\gamma\delta + \gamma\delta + \alpha\delta + \alpha\beta + 1}{\beta\gamma\delta + \delta + \beta}$$

u. s. w.

Daraus geht hervor, dafs, wenn $\frac{m}{n}$, $\frac{p}{q}$ zwei aufeinanderfolgende Resultate sind und μ ein neuer Quotient, das nächstfolgende Resultat

$$\frac{p\mu + m}{q\mu + n}$$

sein wird. Dies ist das **allgemeine Gesetz**, nach welchem man leicht den Wert des gegebenen Kettenbruchs, welches auch die Anzahl seiner Glieder sein möge, berechnen kann.

Das Schema der Rechnung ist folgendes:

Quotienten: $\alpha\,,\ \beta\,,\ \gamma\ \ ,\ \ \delta\ \ ,\ \cdots\ \mu\,,\ \mu'\,,\ \mu''\,,\ \cdots$

Näherungsbrüche: $\frac{1}{0},\ \frac{\alpha}{1},\ \frac{\alpha\beta+1}{\beta},\ \frac{\alpha\beta\gamma+\gamma+\alpha}{\beta\gamma+1},\ \cdots\ \frac{p}{q},\ \frac{p'}{q'},\ \frac{p''}{q''},\ \cdots$

Man schreibe in eine Zeile die aufeinanderfolgenden Quotienten α, β, γ, $\delta\ldots$, setze unter die beiden ersten die beiden Brüche $\frac{1}{0}$, $\frac{\alpha}{1}$ (wo der erste nur deshalb hingesetzt wird, um das Gesetz besser erkennen zu lassen), multipliciere darauf jeden Zähler mit dem darüber stehenden Quotienten und addiere dazu den vorhergehenden Zähler, so ist die Summe der folgende Zähler. Genau ebenso verfahre man hinsichtlich der Nenner. Die Reihe der Brüche, welche sich aus dieser Rechnung ergeben, stellt die verschiedenen Werte des gegebenen Kettenbruches dar, je nachdem man mehr oder weniger Glieder nimmt. Diese Brüche müssen sich mehr und mehr dem vollständigen Werte des Kettenbruches nähern, und dies ist der Grund, weshalb wir sie **Näherungsbrüche** nennen. Erstreckt sich der Kettenbruch nicht ins Unendliche, so wird der letzte der Näherungsbrüche der genaue Wert des gegebenen Kettenbruches sein.

5.

Um das soeben angegebene Gesetz zu begründen, nehmen wir an, dafs es wenigstens bis zu einem gewissen Quotienten μ richtig sei. Ist $\frac{p}{q}$ der Näherungsbruch, welcher dem Quotienten μ entspricht, oder welcher unmittelbar unter diesem steht, ist ferner $\frac{p^0}{q^0}$ der Näherungsbruch, welcher $\frac{p}{q}$ vorangeht, und $\frac{p'}{q'}$ derjenige, welcher auf ihn folgt, nämlich so:

$$\cdots\ \frac{p^0}{q^0},\ \frac{p}{q},\ \frac{p'}{q'},$$

so erhält man dem in Rede stehenden Gesetze zufolge:

$$p' = p\mu + p^0$$
$$q' = q\mu + q^0,$$

und es wird der Bruch $\frac{p'}{q'}$ derjenige sein, welcher sich aus allen Quotienten des Kettenbruches bis zu μ einschliefslich ergiebt. Fügen wir jetzt hinter μ noch einen neuen Quotienten μ' hinzu, und ist $\frac{p''}{q''}$ der bis zum Quotienten μ' einschliefslich berechnete Wert des Kettenbruchs, so ist klar, dafs der analytische Wert von $\frac{p''}{q''}$ nichts

andres ist als der von $\frac{p'}{q'}$, wenn man in letzterem $\mu + \frac{1}{\mu'}$ an Stelle von μ setzt. Folglich erhält man:

$$\frac{p''}{q''} = \frac{p\left(\mu + \frac{1}{\mu'}\right) + p^0}{q\left(\mu + \frac{1}{\mu'}\right) + q^0} = \frac{p'\mu' + p}{q'\mu' + q}.$$

Mithin leitet sich der Näherungsbruch $\frac{p''}{q''}$ aus den beiden vorhergehenden $\frac{p}{q}$, $\frac{p'}{q'}$ und dem dem letzteren entsprechenden Quotienten μ' dem Gesetze:

$$p'' = p'\mu' + p$$
$$q'' = q'\mu' + q$$

gemäfs her. Dieses Fortschreitungsgesetz wird demnach allgemein für die ganze Ausdehnung des Kettenbruches gelten.

6.

Es ist zu beachten, dafs die aufeinanderfolgenden Näherungsbrüche

$$\frac{1}{0}, \ \frac{\alpha}{1}, \ \frac{\alpha\beta + 1}{\beta}, \ \frac{\alpha\beta\gamma + \gamma + \alpha}{\beta\gamma + 1}, \ldots$$

abwechselnd gröfser und kleiner als der vollständige Wert x des Kettenbruches sind. Es ist dies eine Folge davon, dafs die Quotienten α, β, γ, $\delta \ldots$ sämtlich positiv genommen sind. Nimmt man nämlich nur ein Glied α, so ist offenbar $\alpha < x$; nimmt man zwei Glieder, so ist $\alpha + \frac{1}{\beta} > x$, denn man müfste, um den wahren Wert von x zu erhalten, den Nenner β um eine gewisse Gröfse vermehren. Ebenso sieht man, dafs, wenn man drei Glieder $\alpha + \frac{1}{\beta + \frac{1}{\gamma}}$ nimmt, das Resultat kleiner ist als x und so abwechselnd weiter. Folglich:

Der Wert von x ist stets zwischen zwei aufeinanderfolgenden Näherungsbrüchen enthalten.

Nachdem dieses festgestellt ist, behaupte ich, dafs, wenn $\frac{p^0}{q^0}$, $\frac{p}{q}$ zwei aufeinanderfolgende Näherungsbrüche sind, die Gleichung besteht:

$$pq^0 - p^0q = \pm 1,$$

wo das obere Zeichen gilt, wenn der Bruch $\frac{p}{q}$ zu den Brüchen, welche gröfser als x sind, gehört, oder wenn er von ungerader

Ordnung ist (wobei $\frac{1}{0}$ als erster betrachtet wird), und das untere Zeichen, wenn er von gerader Ordnung ist.

Betrachtet man nämlich drei aufeinanderfolgende Näherungsbrüche $\frac{p^0}{q^0}$, $\frac{p}{q}$, $\frac{p'}{q'}$, und bezeichnet man den zu $\frac{p}{q}$ gehörigen Quotienten mit μ, so hat man dem bewiesenen Gesetze zufolge:

$$p' = \mu p + p^0$$
$$q' = \mu q + q^0.$$

Hieraus folgt:

$$p'q - pq' = -(pq^0 - p^0q).$$

Aus demselben Grunde aber erhält man, wenn $\frac{p^{00}}{q^{00}}$ der dem Bruche $\frac{p^0}{q^0}$ vorangehende Näherungsbruch ist:

$$pq^0 - p^0q = -(p^0q^{00} - p^{00}q^0).$$

Geht man also bis auf die beiden ersten Brüche $\frac{1}{0}$, $\frac{\alpha}{1}$, bei welchen die analoge Differenz $1 \cdot 1 - \alpha \cdot 0 = 1$ ist, zurück, so folgt, dafs die Differenz $pq^0 - p^0q$ stets gleich 1 ist und zwar mit dem Vorzeichen $+$ versehen, wenn $\frac{p}{q}$ von ungerader, mit dem Vorzeichen $-$ versehen, wenn es von gerader Ordnung ist.

7.

Wir wollen jetzt untersuchen, welches die Differenz zwischen einem Näherungsbruche $\frac{p}{q}$ und dem vollständigen Werte x des Kettenbruches ist.

Zu dem Zwecke möge stets der $\frac{p}{q}$ vorangehende Näherungsbruch mit $\frac{p^0}{q^0}$ und der diesem entsprechende vollständige Quotient mit y bezeichnet sein. Dann ist dem Bewiesenen zufolge:

$$x = \frac{py + p^0}{qy + q^0}.$$

Hieraus erhält man:

$$x - \frac{p}{q} = \frac{p^0q - pq^0}{q(qy + q^0)} = \frac{\mp 1}{q(qy + q^0)}$$

und:

$$x - \frac{p^0}{q_0} = \frac{(pq^0 - qp^0)y}{q^0(qy + q^0)} = \frac{\pm y}{q^0(qy + q^0)}.$$

Somit erkennt man folgendes:

1) $x - \frac{p}{q}$ und $x - \frac{p^0}{q^0}$ sind immer entgegengesetzten Zeichens und es ist demnach, wie wir schon bewiesen haben, der genaue Wert von x immer zwischen zwei aufeinanderfolgenden Näherungsbrüchen enthalten.

2) Die Differenz $x - \frac{p}{q}$ ist im allgemeinen kleiner als $\frac{1}{q^2}$; dieselbe kann mithin durch $\frac{\pm \delta}{q^2}$, wo δ kleiner als 1 ist, dargestellt werden.

3) Die Gröfse $p - qx$ ist (vom Vorzeichen abgesehen) kleiner als $p^0 - q^0 x$. Denn es ist $\frac{1}{y} = \frac{p - qx}{q^0 x - p^0}$, und y ist, wie aus der Natur der Kettenbrüche folgt, immer gröfser als 1.

Demnach ist umsomehr $\frac{p}{q} - x$ kleiner als $\frac{p^0}{q^0} - x$. Folglich liegt der Näherungsbruch $\frac{p}{q}$ näher an x, als alle vorhergehenden. Diese Eigenschaft rechtfertigt die Benennung dieser Brüche.

8.

Ist jetzt $\frac{\pi}{\varphi}$ irgend ein Bruch, dessen Nenner φ kleiner ist als q, so behaupte ich, dafs die Gröfse $\pi - \varphi x$, vom Vorzeichen abgesehen, gröfser ist als $p - qx$ und selbst gröfser als $p^0 - q^0 x$.

Denn nimmt man:

$$M = p\varphi - q\pi$$
$$N = p^0\varphi - q^0\pi,$$

so ergiebt sich umgekehrt:

$$(pq^0 - p^0 q)\pi = p^0 M - pN$$
$$(pq^0 - p^0 q)\varphi = q^0 M - qN.$$

Nun ist aber nach Voraussetzung $\varphi < q$, und ferner ist $pq^0 - p^0 q = \pm 1$; mithin werden die beiden Zahlen M und N notwendig dasselbe Vorzeichen haben. Nachdem dieses festgestellt ist, erhält man:

$$(pq^0 - p^0 q)(\pi - \varphi x) = M(p^0 - q^0 x) - N(p - qx).$$

Da aber M und N dasselbe Zeichen, die Gröfsen $p^0 - q^0 x$ und $p - qx$ aber entgegengesetztes Zeichen haben und ferner $pq^0 - p^0 q = \pm 1$ ist, so ist $\pi - \varphi x$ nicht allein gröfser als jede der Gröfsen $p^0 - q^0 x$, $p - qx$, sondern auch mindestens gleich ihrer Summe.

Da nun nach Voraussetzung $\varphi < q$ und somit allgemein $\pi - \varphi x > p - qx$ ist, so folgt daraus um so mehr:

$$\frac{\pi}{\varphi} - x > \frac{p}{q} - x.$$

Mithin liegt der Näherungsbruch $\frac{p}{q}$ immer näher an x, als jeder andere Bruch $\frac{\pi}{\varphi}$, dessen Nenner kleiner als q ist.

Diese Eigenschaft der Kettenbrüche kommt jedesmal dann mit Vorteil zur Anwendung, wenn es sich darum handelt, Verhältnisse zwischen sehr grofsen Zahlen oder irrationale Zahlen durch Verhältnisse auszudrücken, welche möglichst einfach sind und den ersteren möglichst nahe kommen.

9.

Ist ein Bruch $\frac{p}{q}$ gegeben, der sich von einer beliebigen Gröfse x um $\pm \frac{\delta}{q^2}$ unterscheidet, worin δ kleiner als die Einheit ist, so soll die Bedingung dafür ermittelt werden, dafs $\frac{p}{q}$ einer der Näherungsbrüche ist, welche sich bei der Entwicklung von x in einen Kettenbruch ergeben.

Dazu setzen wir voraus, dafs die Entwicklung des Bruches $\frac{p}{q}$ die aufeinanderfolgenden Quotienten $\alpha, \beta, \gamma, \ldots \mu$ ergebe, und dafs man mittelst derselben die gegen $\frac{p}{q}$ convergierenden Brüche berechnet habe, nämlich:

Quotienten: $\alpha, \quad \beta, \quad \gamma, \quad \ldots \mu$

Näherungsbrüche: $\frac{1}{0}, \; \frac{\alpha}{1}, \; \frac{\alpha\beta + 1}{\beta}, \ldots \frac{p^0}{q^0}, \; \frac{p}{q}.$

Wenn der Bruch $\frac{p}{q}$ ein Näherungsbruch von x ist, so müssen die Quotienten $\alpha, \beta, \gamma, \ldots \mu$ auch bei der Entwicklung von x sich ergeben, und auf den Quotienten μ müssen noch mehrere andere $\mu', \mu'', \ldots$ folgen. Nennen wir y den vollständigen Quotienten, welcher in der Entwicklung von x dem Näherungsbruche $\frac{p}{q}$ entspricht, so hat man:

$$x = \frac{py + p^0}{qy + q^0},$$

mithin:

$$x - \frac{p}{q} = \frac{p^0 q - p q^0}{q(qy + q^0)} = \frac{\mp 1}{q(qy + q^0)}.$$

Da diese Gröfse gleich $\pm \frac{\delta}{q^2}$ sein soll, so mufs zunächst das Vorzeichen von $pq^0 - p^0q$ mit demjenigen von δ übereinstimmen. Dies läfst sich aber stets erreichen.

Denn da die Reihe der Quotienten $\alpha, \beta, \gamma, \ldots \mu$ aus dem gegebenen Bruche $\frac{p}{q}$ durch dieselbe Rechnung erhalten ist, welche man anwendet, um den gemeinsamen Teiler von p und q zu finden, so ist der letzte dieser Quotienten μ immer gröfser als die Einheit. Denn wäre er gleich 1, so würde der Kettenbruch $\alpha + \frac{1}{\beta + \cdots}$, anstatt mit den beiden Gliedern $\frac{1}{\lambda} + \frac{1}{\mu}$ zu endigen, mit dem einen Gliede $\frac{1}{\lambda + 1}$ aufhören. Umgekehrt kann man also auch, wenn man es für zweckmäfsig hält, den letzten Quotienten μ in zwei andere $\mu - 1, 1$ zerlegen, so dafs man die Berechnung der Näherungsbrüche von $\frac{p}{q}$ nach Belieben auf die eine oder andere der beiden Arten

$$\begin{array}{cccc} \cdots \lambda, & \mu \quad , & \cdots \lambda, & \mu - 1, \; 1 \\ \frac{m}{n}, & \frac{p}{q} & \frac{m}{n} \quad , & \frac{p-m}{q-n}, \; \frac{p}{q} \end{array}$$

als beendigt ansehen kann. Ist $\frac{p^0}{q^0}$ der Näherungsbruch, welcher bei der einen oder andern Annahme unmittelbar $\frac{p}{q}$ vorangeht, so kann man also entweder $p^0 = m$, $q^0 = n$ oder $p^0 = p - m$, $q^0 = q - n$ annehmen. Das Vorzeichen von $pq^0 - p^0q$ ist aber in beiden Fällen entgegengesetzt. Mithin läfst sich in jedem Falle bewirken, dafs die Gröfse $pq^0 - p^0q$ dasjenige Vorzeichen besitzt, welches man will.

Man hat also ohne Zweideutigkeit:

$$\frac{1}{q(qy + q^0)} = \frac{\delta}{q^2}, \text{ oder } \delta = \frac{q}{qy + q^0}.$$

Da nun y positiv und gröfser als 1 sein mufs, wenn y der dem Näherungsbruche $\frac{p}{q}$ entsprechende vollständige Quotient sein soll, so ist:

$$\delta < \frac{q}{q + q^0};$$

und umgekehrt, wenn $\delta < \frac{q}{q + q^0}$ ist, so ist der Wert von y positiv und gröfser als 1, und es wird somit $\frac{p}{q}$ einer der Näherungsbrüche

von x sein. Dies ist die Bedingung, welche gefunden werden sollte.

Diese Bedingung würde unter andern immer erfüllt sein, wenn $\delta < \frac{1}{2}$ wäre, da stets $q^0 < q$ ist.

10.

Wir wollen an dieser Stelle eine Anwendung der vorstehenden Eigenschaft geben, die bei der Auflösung der unbestimmten Gleichungen zweiten Grades von Nutzen sein wird.

Ist $p^2 - Aq^2 = \pm D$ eine unbestimmte Gleichung, in welcher $D < \sqrt{A}$ ist, so behaupte ich, dafs, wenn diese Gleichung auflösbar ist, der Bruch $\frac{p}{q}$ unter den Näherungsbrüchen von $\sqrt{A}$ vorkommt.

In der That erhält man aus dieser Gleichung:

$$p - q\sqrt{A} = \frac{\pm D}{p + q\sqrt{A}}$$

und somit:

$$\frac{p}{q} - \sqrt{A} = \frac{\pm D}{q(p + q\sqrt{A})} = \frac{\pm \delta}{q^2},$$

folglich:

$$\delta = \frac{Dq}{p + q\sqrt{A}}.$$

Ist $\frac{p^0}{q^0}$ der Näherungsbruch, welcher $\frac{p}{q}$ vorangeht, und welcher so bestimmt ist, dafs das Zeichen von δ dasselbe ist wie das von D, so bleibt zu beweisen übrig, dafs

$$\frac{Dq}{p + q\sqrt{A}} < \frac{q}{q + q^0},$$

oder:

$$D(q + q_0) < p + q\sqrt{A}.$$

Setzt man auf der rechten Seite an Stelle von p seinen Wert $q\sqrt{A} \pm \frac{\delta}{q}$, so läfst sich die zu beweisende Ungleichheit folgendermafsen schreiben:

$$(q + q^0)(\sqrt{A} - D) + (q - q^0)\sqrt{A} \pm \frac{\delta}{q} > 0.$$

Diese Ungleichheit ist aber augenscheinlich richtig, da $\sqrt{A} > D$, $q > q^0$ ist und der Teil $(q - q^0)\sqrt{A}$, welcher mindestens gleich $\sqrt{A}$ ist, allein schon $\frac{\delta}{q}$, welches kleiner als die Einheit ist, übersteigt.

Mithin kommt $\frac{p}{q}$ immer unter den Näherungsbrüchen von $\sqrt{A}$ vor, so dafs man, um alle ganzzahligen Lösungen der Gleichung

$$x^2 - Ay^2 = \pm D,$$

in welcher $D < \sqrt{A}$ ist, zu erhalten, nur $\sqrt{A}$ in einen Kettenbruch zu entwickeln und die daraus entstehenden Näherungsbrüche zu berechnen hat.

11.

Betrachten wir einen Kettenbruch $\frac{1}{\alpha + \frac{1}{\beta + \cdots}} = \frac{p}{q}$, welcher kleiner als die Einheit ist und eine endliche Anzahl von Gliedern besitzt, und berechnen wir die Näherungsbrüche in der gewöhnlichen Weise, wie folgt:

Quotienten: $\alpha, \; \beta, \; \gamma, \cdots \varkappa, \; \lambda, \; \mu$

Näherungsbrüche: $\frac{0}{1}, \frac{1}{\alpha}, \frac{\beta}{\alpha\beta + 1}, \cdots \frac{p^{000}}{q^{000}}, \frac{p^{00}}{q^{00}}, \frac{p^0}{q^0}, \frac{p}{q}$,

so erhält man dem Bildungsgesetze zufolge:

$$q = \mu q^0 + q^{00}, \quad \text{und daher:} \quad \frac{q^0}{q} = \frac{1}{\mu + \frac{q^{00}}{q^0}}$$

$$q^0 = \lambda q^{00} + q^{000}, \quad \text{„} \quad \text{„} \quad \frac{q^{00}}{q^0} = \frac{1}{\lambda + \frac{q^{000}}{q^{00}}}$$

$$q^{00} = \varkappa q^{000} + q^{0000}, \quad \text{„} \quad \text{„} \quad \frac{q^{000}}{q^{00}} = \frac{1}{\varkappa + \frac{q^{0000}}{q^{000}}}$$

u. s. w. u. s. w.

Folglich allgemein:

$$\frac{q^0}{q} = \frac{1}{\mu + \frac{1}{\lambda + \frac{1}{\varkappa + \cdots + \frac{1}{\alpha}}}},$$

d. h. die Entwicklung von $\frac{q^0}{q}$ giebt die Quotienten $\mu, \lambda, \varkappa, \ldots \beta, \alpha$, und diese sind nichts andres als die Glieder des gegebenen Kettenbruchs, in umgekehrter Reihenfolge genommen.

Wenn demnach der Fall eintritt, dafs diese Quotienten eine symmetrische Reihe bilden, d. h. eine Reihe wie $\alpha, \beta, \gamma, \ldots \gamma, \beta, \alpha$, in welcher sowohl die beiden äufsersten als auch die von den äufsersten gleichweit abstehenden Glieder einander gleich sind, so ist offenbar $\frac{q^0}{q} = \frac{p}{q}$, oder $q^0 = p$. Ist umgekehrt $q^0 = p$, so

kann man daraus schliefsen, dafs die Reihe der Quotienten symmetrisch ist.

Beispiele von solchen Reihen wird man bei der Kettenbruchentwicklung der Quadratwurzeln aus Zahlen kennen lernen.

§ 2.

Auflösung der unbestimmten Gleichungen ersten Grades.

12.

Sind zwei Zahlen a und b, die **prim** zu einander sind, gegeben, so kann man immer die Gleichung

$$ax - by = 1$$

in **ganzen** Zahlen auflösen.

Zu dem Zwecke mufs man $\frac{a}{b}$ in einen Kettenbruch verwandeln, und die Reihe der Näherungsbrüche von $\frac{a}{b}$ berechnen. Ist $\frac{a^0}{b^0}$ derjenige Näherungsbruch, welcher $\frac{a}{b}$ vorangeht, so hat man die Gleichung:

$$ab^0 - a^0 b = \pm 1.$$

Wenn das Zeichen $+$ gilt, so ist unmittelbar $x = b^0$, $y = a^0$, oder allgemeiner, wenn man eine unbestimmte Zahl z hinzunimmt:

$$x = b^0 + bz$$
$$y = a^0 + az.$$

Ist dagegen $ab^0 - a^0 b = -1$, so kann man $x = -b^0$, $y = -a^0$ setzen, oder allgemeiner:

$$x = -b^0 + bz$$
$$y = -a^0 + az,$$

wo z eine unbestimmte Zahl ist, die man nach Belieben positiv oder negativ nehmen kann.

Allgemein, soll die Gleichung

$$ax - by = c,$$

wo a und b immer zu einander prim sein sollen, aufgelöst werden, so suche man ebenso mit Hülfe der Kettenbrüche die Zahlen a^0 und b^0, welche

$$ab^0 - a^0 b = \pm 1$$

ergeben; dann folgt daraus:

$$x = bz \pm b^0 c$$
$$y = az \pm a^0 c.$$

Mittelst der Unbestimmten z kann man leicht eine solche Lösung finden, daſs x nicht $\pm \frac{1}{2} b$ übersteigt, und eine andere solche, daſs y nicht gröſser ist als $\pm \frac{1}{2} a$. Wenn nämlich $b^0 c$ gröſser ist als $\frac{1}{2} b$, so kann man für z diejenige ganze Zahl nehmen, welche $\frac{b^0 c}{b}$ am nächsten liegt; alsdann ist $b^0 c - bz$ kleiner als $\frac{1}{2} b$.

Wir haben vorausgesetzt, daſs a und b keinen gemeinsamen Teiler haben. Denn hätten sie einen solchen, so würde die Gleichung $ax - by = c$ nicht stattfinden können, wofern nicht c selbst durch diesen gemeinschaftlichen Teiler teilbar wäre, und in diesem Falle würde man ihn durch Division wegschaffen müssen.

Bemerkung. Ohne die Zahlen t und u, welche unbestimmt sein können, zu kennen, darf man immer, wenn man nur weiſs, daſs die eine dieser Zahlen u prim zu einer gegebenen Zahl A ist, annehmen, daſs es zwei Zahlen n und z von solcher Beschaffenheit giebt, daſs $t = nu - Az$ ist, und ferner noch, daſs n nicht gröſser ist als $\frac{1}{2} A$. Diese Eigenschaft wird in der Folge bei vielen Gelegenheiten Anwendung finden.

13.

Die Gleichung $ax - by = c$, die wir soeben aufgelöst haben, giebt das Mittel an die Hand, um einen solchen Wert von x zu bestimmen, daſs $\frac{ax - c}{b}$ eine **ganze** Zahl ist, eine Bedingung, die wir ausdrücken, indem wir setzen:

$$\frac{ax - c}{b} = e \text{ (entier)}.$$

Es kann nun die Aufgabe gestellt sein, daſs mehrere derartige Bedingungen gleichzeitig erfüllt sein sollen. Nehmen wir an, daſs man einen solchen Wert von x verlangt, daſs die drei Gröſsen

$$\frac{ax - c}{b}, \quad \frac{a'x - c'}{b'}, \quad \frac{a''x - c''}{b''}$$

ganze Zahlen seien, so giebt die erste Bedingung einen Wert von x von der Form $x = m + bz$. Setzt man diesen Wert in die zweite Gröſse ein, so muſs man z derart bestimmen, daſs

$$\frac{a'bz + a'm - c'}{b'} = e$$

ist. Hier kann es eintreffen, daſs die Lösung unmöglich ist. Denn wenn b und b' einen gemeinschaftlichen Teiler ϑ haben, so ist klar,

dafs die vorstehende Gleichung nicht stattfinden kann, wofern nicht die bestimmte Zahl $a'm - c'$ ebenfalls durch ϑ teilbar ist.

Im allgemeinen wird der Wert von z, welcher der vorhergehenden Bedingung (falls sie nicht unmöglich ist) genügt, von der Form sein: $z = n + b'z'$ oder $z = n + \frac{b'}{\vartheta} z'$, wenn b' und b einen gemeinschaftlichen Teiler ϑ haben. Man erhält also im allgemeinen $x = m' + B'z'$, wo B' gleich bb' oder gleich der kleinsten Zahl ist, die gleichzeitig durch b und b' teilbar ist. Wird dieser Wert in die dritte Gröfse, welche eine ganze Zahl werden sollte, eingesetzt, so ergiebt sich daraus der schliefsliche Wert von x, welcher von der Form $x = M + Bz$ sein wird, wo B die kleinste, gleichzeitig durch b, b', b'' teilbare ganze Zahl und z eine unbestimmte Zahl ist. Auf diese Weise wird man immer einen Wert von x finden können, der kleiner oder wenigstens nicht gröfser als $\frac{1}{2}B$ ist. Aus diesem ersten Werte leitet man dann alle andern her, indem man ein beliebiges Vielfache von B zu ihm addiert oder von ihm subtrahiert.

Wenn die Zahlen, mit denen man rechnet, nicht sehr grofs sind, ist es leicht, den verschiedenen Bedingungen zu genügen, ohne die Kettenbrüche zu Hülfe zu nehmen. Wir wollen z. B. eine Zahl x von der Beschaffenheit suchen, dafs die drei Gröfsen:

$$\frac{3x - 10}{7}, \quad \frac{11x + 8}{17}, \quad \frac{16x - 1}{5}$$

ganze Zahlen werden. Die letzte Gröfse enthält einen ganzen Teil $3x$ und einen Rest $\frac{x-1}{5}$. Ist dieser Rest gleich z, so hat man:

$$x = 5z + 1.$$

Wird dieser Wert, welcher der dritten Bedingung genügt, in den ersten Ausdruck eingesetzt, so erhält man

$$\frac{15z - 7}{7},$$

oder, wenn man den ganzen Teil wegläfst, $\frac{z}{7} = e$, also:

$$z = 7u \text{ und } x = 35u + 1.$$

Diesen Wert hat man noch in die zweite Gröfse zu substituieren, wodurch man erhält:

$$\frac{385u + 19}{17} = e.$$

Läfst man den in der linken Seite enthaltenen ganzen Teil weg, so wird diese Bedingung:

$$\frac{11u + 2}{17} = e \text{ oder } \frac{-6u + 2}{17} = e.$$

Multipliciert man die linke Seite mit 3 und läfst man den ganzen Teil weg, so erhält man:

$$\frac{-u + 6}{17} = e.$$

Mithin:

$$u = 6 + 17t \text{ und } x = 211 + 5 \cdot 7 \cdot 17t.$$

Man sieht hieraus, dafs die kleinste Zahl, welche der Aufgabe genügt, 211 ist.

14.

Jeder Bruch $\frac{C}{D}$, dessen Nenner das **Produkt zweier** zu einander **primen** Zahlen m und n ist, läfst sich in zwei andre Brüche zerlegen, welche m und n zu Nennern haben.

Sind nämlich m und n prim zu einander, so kann man immer der Gleichung $mx + ny = C$ genügen und daraus folgt:

$$\frac{C}{D} = \frac{C}{mn} = \frac{x}{n} + \frac{y}{m}.$$

Jeden dieser Brüche kann man weiter in zwei andere zerlegen, wenn sein Nenner das Produkt zweier zu einander primen Zahlen ist. Allgemein also kann jeder Bruch $\frac{C}{D}$, dessen Nenner das Produkt von mehreren zu einander primen Zahlen $m, n, p, ..$ ist, in mehrere andere zerlegt werden, deren Nenner die einzelnen Faktoren $m, n, p, \ldots$ sind, und die Aufgabe wird immer unbestimmter werden, je mehr die Anzahl der Faktoren zunimmt.

§ 3.

Methode, um die unbestimmten Gleichungen zweiten Grades in rationalen Zahlen aufzulösen.

15.

Ist die allgemeine Gleichung

$$ax^2 + bxy + cy^2 + dx + ey + f = 0$$

gegeben, in welcher x und y unbestimmte Zahlen und a, b, c, d, e, f gegebene positive oder negative ganze Zahlen sind, so erhält man zunächst aus dieser Gleichung:

$$2ax + by + d = \sqrt{(by + d)^2 - 4a(cy^2 + ey + f)}.$$

Setzt man sodann zur Abkürzung die Wurzelgröfse gleich t und ferner:

$$b^2 - 4ac = A$$
$$bd - 2ae = g$$
$$d^2 - 4af = h,$$

so hat man die beiden Gleichungen:

$$2ax + by + d = t$$
$$Ay^2 + 2gy + h = t^2.$$

Multiplicieren wir die letztere mit A und setzen wieder:

$$Ay + g = u$$
$$g^2 - Ah = B,$$

so erhalten wir die transformierte Gleichung:

$$u^2 - At^2 = B.$$

Umgekehrt, wenn man Werte von u und t finden kann, welche der Gleichung $u^2 - At^2 = B$ genügen, so erhält man daraus für die gegebene Gleichung die Werte der unbestimmten Zahlen x und y, nämlich:

$$y = \frac{u - g}{A}, \quad x = \frac{t - by - d}{2a},$$

wobei zu beachten ist, dafs u und t beide mit einem beliebigen Vorzeichen genommen werden können.

Wenn man die Lösung der gegebenen Gleichung in rationalen Zahlen haben will, so hat man nur die transformierte Gleichung $u^2 - At^2 = B$ für solche Zahlen aufzulösen. Wenn man aber die gegebene Gleichung in ganzen Zahlen auflösen will, so ist erforderlich, nicht allein, dafs t und u ganze Zahlen seien, sondern auch, dafs die Werte von t und u, in die von x und y eingesetzt, für diese ganze Zahlen ergeben. An dieser Stelle werden wir uns nur mit der Auflösung in **rationalen** Zahlen beschäftigen.

16.

Jede unbestimmte Gleichung zweiten Grades läfst sich, wie wir eben gesehen haben, auf die Form $u^2 - At^2 = B$ zurückführen. Nun kann man, welches auch die rationalen Zahlen t und u sein mögen, annehmen, dafs sie auf einen und denselben Nenner gebracht sind. Folglich wird man, wenn man $u = \frac{x}{z}$, $t = \frac{y}{z}$ setzt, die Gleichung aufzulösen haben:

$$x^2 - Ay^2 = Bz^2,$$

in welcher jetzt x, y, z ganze Zahlen sind.



Man kann voraussetzen, dafs diese drei Zahlen unter einander keinen allen gemeinschaftlichen Teiler haben; denn hätten sie einen solchen, so könnte man ihn durch Division wegschaffen. Ebenso kann man voraussetzen, dafs die Zahlen A und B keinen quadratischen Teiler haben. Denn wäre z. B. $A = A'k^2$, $B = B'l^2$, so könnte man $ky = y'$ und $lz = z'$ setzen, und dadurch würde die aufzulösende Gleichung werden:

$$x'^2 - A'y'^2 = B'z'^2,$$

in welcher A' und B' keinen quadratischen Teiler mehr haben.

Wenn die Gleichung $x^2 - Ay^2 = Bz^2$ in dieser Weise vorbereitet ist, so wird man bemerken, dafs irgend zwei der unbestimmten Zahlen x, y, z einen gemeinschaftlichen Teiler nicht haben können. Denn wenn z. B. x^2 und y^2 durch ϑ^2 teilbar wären, so müfste auch Bz^2 durch ϑ^2 teilbar sein. Nun läfst sich aber z^2 nicht durch ϑ^2 teilen, da die drei Zahlen x, y, z keinen gemeinschaftlichen Teiler haben; ebensowenig aber läfst sich B durch ϑ^2 teilen, da B keinen quadratischen Faktor besitzt. Mithin sind x und y prim zu einander. Aus demselben Grunde sind auch x und z, sowie y und z zu einander prim.

Ich behaupte ferner, dafs A und B **positiv** angenommen werden dürfen. Denn hinsichtlich der Vorzeichen der Glieder unserer Gleichung lassen sich nur die folgenden drei Kombinationen machen:

$$x^2 - Ay^2 = + Bz^2$$
$$x^2 - Ay^2 = - Bz^2$$
$$x^2 + Ay^2 = + Bz^2.$$

(Die Kombination $x^2 + Ay^2 = - Bz^2$ ist weggelassen, weil dieselbe, wie man sieht, unerfüllbar ist.)

Von diesen drei Kombinationen fällt die zweite mit der dritten durch eine einfache Umformung zusammen. Denn multipliciert man die letztere mit B und setzt dann $Bz = z'$, $AB = A'$, so erhält man:

$$z'^2 - A'y^2 = Bx^2.$$

Somit kann die aufzulösende Gleichung stets auf die Form

$$x^2 - By^2 = Az^2$$

gebracht werden, in welcher A und B positive Zahlen ohne jeden quadratischen Teiler sind.

17.

Das Verfahren, welches wir anwenden werden, um diese Gleichung aufzulösen, ist von Lagrange in den Abhandlungen

der Berliner Akademie vom Jahre 1767 angegeben worden. Es besteht darin, dafs man durch Transformationen die Koefficienten A und B nach und nach zu verkleinern sucht, bis einer dieser Koefficienten gleich 1 ist, in welchem Falle dann die Auflösung sich unmittelbar aus bekannten Formeln ergiebt.

Die in dieser Weise umgeformte Gleichung ist nämlich von der Form $x^2 - y^2 = Az^2$ oder $x^2 - By^2 = z^2$. Da aber diese beiden Formeln nur eine und dieselbe bilden, so reicht es hin, wenn wir die Auflösung der ersten

$$x^2 - y^2 = Az^2$$

angeben. Zu diesem Zwecke zerlegen wir A in zwei Faktoren α, β (welche stets prim zu einander sein werden, da A keinen quadratischen Teiler hat), und denken uns z ebenfalls in zwei Faktoren p, q zerlegt, so dafs

$$A = \alpha\beta, \quad z = pq$$

ist. Alsdann erhält man die Gleichung:

$$(x + y)(x - y) = \alpha\beta p^2 q^2,$$

welcher man allgemein genügt, wenn man

$$x + y = \alpha p^2, \quad x - y = \beta q^2$$

setzt. Dadurch ergiebt sich:

$$x = \frac{\alpha p^2 + \beta q^2}{2}, \quad y = \frac{\alpha p^2 - \beta q^2}{2}, \quad z = pq,$$

so dafs also die drei unbestimmten Zahlen x, y, z mittelst zweier anderen willkürlichen Zahlen p und q ausgedrückt sind. Träte der Fall ein, dafs die Werte von x und y den Bruch $\frac{1}{2}$ enthielten, so könnte man alle drei Gröfsen x, y, z mit 2 multiplicieren.

Dies ist die **allgemeine** Auflösung der Gleichung:

$$x^2 - y^2 = Az^2.$$

Dieselbe umfafst ebensoviele besondere Formeln, als es verschiedene Arten der Zerlegung von A in zwei Faktoren giebt.

Ist z. B. $A = 30$, so giebt es vier verschiedene Arten, um 30 in zwei Faktoren zu zerlegen, nämlich:

$$1 \cdot 30, \quad 2 \cdot 15, \quad 3 \cdot 10, \quad 5 \cdot 6,$$

und aus diesen ergeben sich folgende vier Auflösungen der Gleichung $x^2 - y^2 = 30z^2$:

$$\begin{aligned}
&1)\quad x = p^2 + 30q^2, \quad y = p^2 - 30q^2, \quad z = 2pq\\
&2)\quad x = 2p^2 + 15q^2, \quad y = 2p^2 - 15q^2, \quad z = 2pq\\
&3)\quad x = 3p^2 + 10q^2, \quad y = 3p^2 - 10q^2, \quad z = 2pq\\
&4)\quad x = 5p^2 + 6q^2, \quad y = 5p^2 - 6q^2, \quad z = 2pq.
\end{aligned}$$

18.

Wir gehen jetzt zur allgemeinen Gleichung

$$x^2 - By^2 = Az^2$$

über und bemerken zunächst, dafs man, da diese Gleichung dieselbe ist, wie $x^2 - Az^2 = By^2$, ohne die Allgemeinheit zu beeinträchtigen, voraussetzen darf, dafs der Koefficient der **rechten** Seite **der gröfsere** von beiden sei. Im Falle sie gleich sein sollten, führt die Reduktion, die wir angeben werden, stets zum Ziele.

Es sei also die Gleichung gegeben:

$$x^2 - By^2 = Az^2,$$

in welcher $A > B$ und ferner A und B positiv und ohne jeden quadratischen Faktor vorausgesetzt werden.

Wie wir bereits bewiesen haben, sind x und y prim zu einander. Daraus folgt, dafs auch y und A prim zu einander sind; denn wenn y^2 und A einen gemeinschaftlichen Teiler ϑ hätten, so müfste x^2 ebenfalls durch ϑ teilbar sein, und es würden somit x^2 und y^2 nicht prim zu einander sein.

Da aber y und A prim zu einander sind, so wird man auch, wenn man voraussetzt, dafs die gegebene Gleichung auflösbar sei, und dafs man somit bestimmte Werte von x und y, z. B. $x = M$, $y = N$ wirklich finden könne, (nach Nr. 12) der Gleichung ersten Grades

$$M = nN - y'A$$

genügen können, wobei M, N, A gegebene zu einander prime Zahlen und n, y' zwei unbestimmte Zahlen wären.

Man kann daher allgemein, ohne diese besonderen Lösungen $x = M$, $y = N$ zu kennen,

$$x = ny - Ay'$$

setzen, wo n und y' zwei unbestimmte Zahlen sind, und setzt man diesen Wert in die gegebene Gleichung ein, so erhält man, nachdem man sie durch A dividiert hat:

$$\left(\frac{n^2 - B}{A}\right) y^2 - 2nyy' + Ay'^2 = z^2.$$

Da nun y und A prim zu einander sind, so kann diese Gleichung nur dann bestehen, wenn $\frac{n^2 - B}{A}$ gleich einer ganzen Zahl ist. Ist diese ganze Zahl gleich $A'k^2$, wo k^2 der gröfste quadratische Teiler derselben sein soll, so ist:

$$n^2 - B = AA'k^2,$$

und die aufzulösende Gleichung wird:

$$A'k^2y^2 - 2nyy' + Ay'^2 = z^2.$$

Wir werden später die einfachsten Hülfsmittel angeben, welche zur Bestimmung einer Zahl n von der Beschaffenheit führen, dafs $\frac{n^2 - B}{A}$ eine ganze Zahl wird. Für jetzt genügt es zu bemerken, dafs, wenn es irgend einen solchen Wert von n, dafs $n^2 - B$ durch A teilbar wird, giebt, dieser Wert um ein beliebiges Vielfaches von A vermehrt oder vermindert werden kann, ohne dafs $n^2 - B$ aufhört, durch A teilbar zu sein. Demnach kann man annehmen, dafs der betreffende Wert zwischen den Grenzen 0 und A oder sogar zwischen den noch engeren Grenzen $-\frac{1}{2}A$ und $+\frac{1}{2}A$ enthalten ist.

Daraus ergiebt sich, dafs, wenn man für n der Reihe nach alle ganzen Zahlen von $-\frac{1}{2}A$ bis $+\frac{1}{2}A$ nimmt, man notwendig einen oder mehrere finden wird, für welche $n^2 - B$ durch A teilbar ist, vorausgesetzt, dafs die Gleichung auflösbar ist; und in dem Falle, wo für keine dieser Zahlen $n^2 - B$ durch A teilbar ist, wird man mit Sicherheit schliefsen können, dafs die gegebene Gleichung nicht auflösbar ist.

19.

Nehmen wir also an, dafs man einen oder mehrere Werte von n, welche die erforderliche Eigenschaft besitzen, gefunden habe, so mufs man mit jedem dieser Werte die Rechnung in folgender Weise weiterführen.

Wir nehmen die Gleichung

$$A'k^2y^2 - 2nyy' + Ay'^2 = z^2$$

wieder auf. Multipliciert man sie mit $A'k^2$, und setzt man zur Abkürzung:

$$A'k^2y - ny' = x', \quad kz = z',$$

so wird die transformierte Gleichung:

$$x'^2 - By'^2 = A'z'^2.$$

Diese transformierte Gleichung würde aufgelöst sein, wenn man die Auflösung der gegebenen Gleichung wüfste, da die Werte von x', y', z' sich leicht aus denen von x, y, z ergeben. Umgekehrt wird die gegebene Gleichung aufgelöst sein, wenn man die Lösung der transformierten gefunden hat. Denn aus den bekannten Werten von x', y', z' kann man gleichfalls die Werte von x, y, z ableiten. Dabei thut es nichts zur Sache, ob diese letzeren ganze oder gebrochene Zahlen sind, da es sich nur um die Auflösung in rationalen Zahlen handelt, und da man, nachdem man irgendwelche gebrochenen Werte von x, y, z gefunden hat, dieselben auf den nämlichen Nenner bringen und sodann den gemeinsamen Nenner weglassen kann.

Da man die Zahl $n < \frac{1}{2}A$ annehmen kann, so wird offenbar $\frac{n^2 - B}{Ak^2}$ oder A' kleiner als $\frac{1}{4}A$ und zugleich positiv sein. Denn es kann nicht $n < \sqrt{B}$ sein, da sonst $n^2 - B < B$ wäre und daher nicht durch A teilbar sein könnte. Mithin ist die gegebene Gleichung auf eine ganz ähnliche Gleichung zurückgeführt, in welcher der Koefficient A', welcher die Stelle von A einnimmt, kleiner als $\frac{1}{4}A$ ist.

20.

Wenn A' noch gröfser als B ist, so kann man in analoger Weise aus der Gleichung $x'^2 - By'^2 = A'z'^2$ eine zweite transformierte Gleichung

$$x''^2 - By''^2 = A''z''^2$$

ableiten, in welcher $A'' < \frac{1}{4}A'$ und stets positiv ist. Um diese zweite transformierte Gleichung zu erhalten, ist keine neue Bedingung weiter zu erfüllen. Denn setzt man, nachdem man bereits

$$\frac{n^2 - B}{A'} = Ak^2$$

gefunden hat, $n = \mu A' + n'$ und nimmt die unbestimmte Zahl μ so an, dafs $n' < \frac{1}{2}A'$ ist, so sieht man leicht, dafs $\frac{n'^2 - B}{A'}$ eine ganze positive Zahl und kleiner als $\frac{1}{4}A'$ ist. Man wird also setzen:

$$n'^2 - B = A'A''k'^2,$$

wo $A'' < \frac{1}{4}A'$ ist und keinen quadratischen Faktor enthält.

Tritt der Fall ein, dafs A'' noch gröfser ist als B, so setze man

dieses System der transformierten Gleichungen, in denen B konstant bleibt, fort, bis man eine Gleichung

$$x^2 - By^2 = Cz^2$$

findet, in welcher C positiv und kleiner als B ist.

21.

Nachdem man jedoch das Glied, welches den gröfseren Koefficienten hat, auf die rechte Seite gebracht hat, wodurch sich

$$x^2 - Cz^2 = By^2$$

ergiebt, kann man in analoger Weise den Koefficienten B mittelst eines zweiten Systems von transformierten Gleichungen

$$x'^2 - Cz'^2 = B'y'^2$$
$$x''^2 - Cz''^2 = B''y''^2$$
u. s. w.

reducieren, wobei die Koefficienten B', B'', ... positiv sind und mindestens im Verhältnis von 4 zu 1 abnehmen. Auf diese Weise wird man bald zu einer transformierten Gleichung

$$x^2 - Cz^2 = Dy^2$$

gelangen, in welcher der Koefficient D kleiner ist als C.

Nun kann die Reihe der positiven und abnehmenden Zahlen A, B, C, D, ... nicht ins Unendliche hin fortgehen; sie mufs vielmehr notwendig mit der Einheit endigen. Ist man zu diesem Gliede gelangt, so ergiebt die Auflösung der letzten transformierten Gleichung, welche ohne weiteres gegeben ist, auch die Auflösung aller vorhergehenden und somit die der gegebenen Gleichung.

Diese Methode ist hier nicht etwa deshalb gegeben worden, weil sie die einfachste oder kürzeste wäre, vermittelst deren man zur wirklichen Auflösung der gegebenen Gleichung gelangen könnte. Aber der Gang, den sie vorschreibt, um die Koefficienten allmählich zu verkleinern, ist sehr deutlich und klar; wir werden daraus bald einen allgemeinen Satz über die Auflösbarkeit der unbestimmten Gleichungen zweiten Grades ableiten.

22.

Es dürfte angebracht sein, einer Schwierigkeit vorzubeugen, die eintreten könnte, wenn beide Koefficienten gleich sind.

Es sei also $A = B$. In diesem Falle scheint es, als ob man, wenn man bewirken will, dafs $\frac{n^2 - B}{A}$ eine ganze Zahl sei, $n = 0$

setzen dürfe. Dann würde $A'k^2 = -1$ oder $A' = -1$ sein, was nicht im Einklang steht mit der Annahme, dafs A' immer positiv genommen werden solle. Indessen ist diese Schwierigkeit leicht zu beseitigen. Denn nimmt man $n = A$ an Stelle von $n = 0$, so erhält man $\frac{n^2 - A}{A} = A - 1$, und dies würde der Wert von $A'k^2$ sein. Man sieht also, dafs die Gleichung

$$x^2 - Ay^2 = Az^2$$

die transformierte Gleichung

$$x'^2 - Ay'^2 = A'z'^2$$

liefert, wo $A' < A$ und positiv ist. Man würde ebenso zu verfahren haben, wenn man im Verlauf der Rechnung $C = B$, oder $D = C$ u. s. w. fände.

Diese Bemerkung zeigt, dafs für den Fall $A = B$ und für andre ähnliche Fälle die Methode nicht minder anwendbar bleibt, und dafs sie somit alle erforderliche Allgemeinheit besitzt. Übrigens läfst sich der in Rede stehende Fall auf einfachere und direktere Weise behandeln. Denn hat man die Gleichung:

$$x^2 - Ay^2 = Az^2,$$

so sieht man zunächst, dafs x teilbar sein mufs durch A. Demnach kann man $x = Au$ setzen und erhält dann:

$$y^2 + z^2 = Au^2.$$

In dieser Gleichung sind z und A zu einander prim (denn andernfalls würden y und z es nicht sein). Somit kann man setzen:

$$y = nz + Ay'.$$

Dies giebt:

$$\frac{n^2 + 1}{A} z^2 + 2nzy' + Ay'^2 = u^2.$$

Diese Gleichung kann nicht bestehen, wofern nicht $\frac{n^2 + 1}{A}$ eine ganze Zahl ist. Nennt man diese ganze Zahl $A'k^2$, wo k^2 der gröfste quadratische Teiler derselben ist, so erhält man:

$$A'k^2z^2 + 2nzy' + Ay'^2 = u^2.$$

Multipliciert man beiderseits mit $A'k^2$ und setzt man:

$$k^2A'z + ny' = z', \quad ku = u',$$

so wird:

$$z'^2 + y'^2 = A'u'^2,$$

so dafs die gegebene Gleichung $y^2 + z^2 = Au^2$ auf eine Gleichung von derselben Form zurückgeführt ist, in welcher A' positiv und

kleiner als $\frac{1}{4}A + \frac{1}{A}$ ist. Führt man mit diesen Transformationen so fort, so wird die Reihe der positiven und abnehmenden Zahlen $A, A', A'', \ldots$ notwendig als letztes Glied die Einheit haben, und da alsdann die letzte Gleichung ohne weiteres auflösbar ist, so wird sich daraus die Lösung aller vorhergehenden ergeben. In diesem Falle existiert keine andere Bedingung für die Möglichkeit der Auflösung der Gleichung, als dafs $\frac{n^2+1}{A} = e$ sein mufs. Alle andern sind eine Folge dieser Bedingung.

Bei der allgemeinen Auflösung dagegen mufs man aufser der ersten Bedingung $\frac{n^2 - B}{A} = e$, so oft man von einem System von transformierten Gleichungen zu einem andern Systeme übergeht, auch den verschiedenen Bedingungen $\frac{n'^2 - C}{B} = e$, $\frac{n''^2 - D}{C} = e$ u. s. w. genügen können. Dies werden wir im folgenden Paragraphen des Näheren untersuchen.

§ 4.

Satz, mit dessen Hülfe man über die Möglichkeit oder Unmöglichkeit der Auflösung einer jeden unbestimmten Gleichung zweiten Grades entscheiden kann.

23.

Im vorhergehenden Paragraphen haben wir gezeigt, dafs sich jede unbestimmte Gleichung zweiten Grades zurückführen läfst auf die Form:

$$x^2 - By^2 = Az^2,$$

in welcher A und B positive ganze Zahlen ohne jeden quadratischen Teiler sind, und in der man überdies $A > B$ annehmen kann.

Nachdem dieses festgestellt ist, mufs man, um zur Auflösung zu gelangen, zunächst eine Zahl α bestimmen, welche kleiner als $\frac{1}{2}A$ und von der Beschaffenheit ist, dafs $\frac{\alpha^2 - B}{A}$ eine ganze Zahl wird.

Ist diese Zahl gefunden, so bildet man die Reihe von Gleichungen:

$$\begin{aligned}
&\alpha^2 - B = AA'k^2, && \\
&\alpha'^2 - B = A'A''k'^2, && \alpha' = \mu A' \pm \alpha < \tfrac{1}{2}A' \\
&\alpha''^2 - B = A''A'''k''^2, && \alpha'' = \mu' A'' \pm \alpha' < \tfrac{1}{2}A'' \\
&\quad \text{u. s. w.} && \quad \text{u. s. w.}
\end{aligned}$$

In der ersten ist $A'k^2$ der Quotient, der sich bei der Division von $\alpha^2 - B$ durch A ergiebt, und k^2 ist die gröfste Quadratzahl, welche in $A'k^2$ aufgeht, so dafs A' nur noch einfache Faktoren enthält, ebenso wie A und B. Dasselbe hat man bei den andern analogen Werten zu beachten. Ist A' bestimmt, so erhält man α' durch die Gleichung $\alpha' = \mu A' \pm \alpha$, wobei die unbestimmte Zahl μ derart zu wählen ist, dafs $\alpha' < \frac{1}{2} A'$ wird (das Zeichen $<$ schliefst den Fall der Gleichheit nicht aus). Ist α' bekannt, so ist $\alpha'^2 - B$ notwendig teilbar durch A'. Den Quotienten bezeichnet man mit $A''k'^2$ und bildet dann ebenso weiter die andern Gleichungen.

Wenn man die Rechnung in dieser Weise anstellt, so wird die Reihe $A, A', A'', \ldots$, bei welcher jedes Glied positiv und kleiner als der vierte Teil des vorhergehenden ist, sehr schnell abnehmen, bis man zu einem Gliede $A^{(n)}$ oder C gelangt, welches kleiner ist als B. Die gegebene Gleichung wird also nach und nach in die folgenden Gleichungen (in denen ich der gröfseren Einfachheit wegen die unbestimmten Zahlen ohne Accente lasse) transformiert sein:

$$x^2 - By^2 = A'z^2$$
$$x^2 - By^2 = A''z^2$$
$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$$
$$x^2 - By^2 = Cz^2,$$

Gleichungen, die derart unter einander zusammenhängen, dafs, wenn die Lösung einer einzigen von ihnen bekannt ist, unmittelbar auch die aller übrigen und somit auch die der vorgelegten Gleichung gegeben ist.

Bei diesem ersten System von transformierten Gleichungen hat man nur eine einzige Bedingung zu erfüllen, nämlich die erste, dafs $\frac{n^2 - B}{A} = e$ sei.

Bringt man aber, weil $C < B$ ist, die letzte transformierte Gleichung auf die Form:

$$x^2 - Cz^2 = By^2,$$

so mufs man, wenn dieselbe auflösbar sein soll, eine Zahl ϑ von der Beschaffenheit finden können, dafs $\vartheta^2 - C$ teilbar ist durch B. Ist diese Bedingung erfüllt, so wird man die Verkleinerung von B mittelst eines zweiten Systems von transformierten Gleichungen

$$x^2 - Cz^2 = B'y^2$$
$$x^2 - Cz^2 = B''y^2$$
$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$$
$$x^2 - Cz^2 = Dy^2$$

in Angriff nehmen, wobei die Reihe $B, B', B'' \ldots$ soweit fortgesetzt ist, bis man zu einem Gliede $D < C$ kommt.

In dieser Weise setze man die Reihe der abnehmenden ganzen Zahlen $A, B, C, D \ldots$ so lange fort, bis man zu einem Gliede, welches gleich der Einheit ist, gelangt. Alsdann ist die Aufgabe gelöst.

24.

Es ist leicht zu sehen, dafs man im Verlaufe dieser Rechnung nirgends Halt zu machen gezwungen ist, wenn man mit Bezug auf eine beliebige transformierte Gleichung

$$x^2 - Fy^2 = Gz^2$$

den beiden Bedingungen

$$\frac{\lambda^2 - F}{G} = e, \quad \frac{\mu^2 - G}{F} = e$$

genügen kann.

Ich behaupte nun, dafs, wenn diese beiden Bedingungen bei der gegebenen Gleichung $x^2 - By^2 = Az^2$ und bei ihrer ersten transformierten Gleichung $x^2 - By^2 = A'z^2$ erfüllt sind, dies auch bei allen andern der Fall sein wird, so dafs also dann die gegebene Gleichung notwendigerweise auflösbar ist.

Setzt man somit voraus, dafs die beiden angegebenen Bedingungen bei den beiden ersten Gleichungen

$$x^2 - By^2 = Az^2$$
$$x^2 - By^2 = A'z^2$$

erfüllt seien, d. h. dafs es derartige ganze Zahlen $\alpha, \beta, \alpha', \beta'$ gebe, für welche

$$\frac{\alpha^2 - B}{A}, \quad \frac{\alpha'^2 - B}{A'}, \quad \frac{\beta^2 - A}{B}, \quad \frac{\beta'^2 - A'}{B}$$

ganze Zahlen werden, so ist zu beweisen, dafs die analogen Bedingungen auch bei der folgenden transformierten Gleichung

$$x^2 - By^2 = A''z^2$$

erfüllt sind. Da man nun bereits $\frac{\alpha''^2 - B}{A''} = A'''k''^2$ hat, so genügt es zu zeigen, dafs es eine ganze Zahl β'' giebt, für welche

$$\frac{\beta''^2 - A''}{B} = e$$

ist.

Bezeichnet ϑ eine der Primzahlen, welche B teilen, so hat man bereits nach den gegebenen Bedingungen:

$$\frac{\beta^2 - A}{\vartheta} = e, \quad \frac{\beta'^2 - A'}{\vartheta} = e.$$

Wir suchen demgemäſs eine Zahl λ, für welche

$$\frac{\lambda^2 - A''}{\vartheta} = e$$

ist. Wenn A'' teilbar ist durch ϑ, so hat dies keine Schwierigkeit. Es sei also A'' nicht durch ϑ teilbar. Dann unterscheiden wir zwei Fälle, je nachdem A' durch ϑ teilbar ist oder nicht.

1) Wenn ϑ ein Teiler ist von A', so wird es auch den Gleichungen

$$\alpha^2 - B = AA'k^2, \quad \alpha' = \mu A' \pm \alpha$$

zufolge ein Teiler von α und α' sein. Ferner hat man:

$$A''k'^2 = \frac{\alpha'^2 - B}{A'} = \frac{(\mu A' \pm \alpha)^2 - B}{A'} = \mu^2 A' \pm 2\mu\alpha + Ak^2.$$

Mithin ist

$$\frac{Ak^2 - A''k'^2}{\vartheta}$$

eine ganze Zahl. Addiert man hierzu:

$$\frac{\beta^2 k^2 - Ak^2}{\vartheta},$$

welches ebenfalls eine ganze Zahl ist, so erhält man:

$$\frac{\beta^2 k^2 - A''k'^2}{\vartheta} = e.$$

k' ist aber prim zu B und folglich auch zu ϑ. Denn hätten k' und B einen gemeinschaftlichen Teiler, so müſste, der Gleichung

$$\alpha'^2 - B = A'A''k'^2$$

zufolge, B einen quadratischen Faktor haben, was der Voraussetzung widerspricht. Man kann somit

$$k\beta = nk' - m\vartheta$$

setzen und erhält:

$$\frac{n^2 k'^2 - A''k'^2}{\vartheta} = e$$

oder einfach:

$$\frac{n^2 - A''}{\vartheta} = e.$$

2) Ist ϑ kein Teiler von A' und somit auch kein Teiler von β', so ergiebt sich aus der Gleichung $\frac{\beta'^2 - A'}{\vartheta} = e$ zunächst:

$$\frac{A'' k'^2 \beta'^2 - A' A'' k'^2}{\vartheta} = e$$

oder:

$$\frac{A'' k'^2 \beta'^2 - \alpha'^2}{\vartheta} = e.$$

Ferner kann man, da $\beta' k'$ und ϑ prim zu einander sind,

$$\alpha' = n \beta' k' - m \vartheta$$

setzen und dies giebt:

$$\frac{n^2 - A''}{\vartheta} = e.$$

Aus diesem Beweise, der für alle Primfaktoren von B gilt, erkennt man, dafs nicht nur die Gleichung $\frac{\beta''^2 - A''}{B} = e$ möglich ist, sondern dafs man den Wert von β'' auch leicht a priori finden kann. Demnach wird keine der Gleichungen

$$x^2 - By^2 = A'' z^2, \; x^2 - By^2 = A''' z^2, \; \ldots,$$

in denen B dasselbe bleibt, unmöglich.

Wir werden jetzt zeigen, dafs dasselbe bei dem zweiten System von transformierten Gleichungen stattfindet, bei welchem C einen und denselben Wert, B dagegen die abnehmende Reihe B', B'' ... durchläuft.

25.

Sind die beiden letzten Gleichungen des ersten Systems:

$$x^2 - By^2 = A^{n-1} z^2$$
$$x^2 - By^2 = A^n z^2 = C z^2,$$

(wobei $n-1$ und n Indices, aber nicht Exponenten sind), so kann man voraussetzen, dafs diese Gleichungen bereits den Bedingungen

$$\frac{\alpha^2 - B}{A^{n-1}} = e, \quad \frac{\beta^2 - A^{n-1}}{B} = e, \quad \frac{\alpha'^2 - B}{A^n} = e, \quad \frac{\beta'^2 - A^n}{B} = B' f^2$$

genügen; alsdann hat man zu beweisen, dafs man bei der folgenden transformierten Gleichung

$$x^2 - A^n y^2 = B' z^2$$

(welche zum zweiten System gehört) den beiden Bedingungen

$$\frac{\varphi^2 - A^n}{B'} = e, \quad \frac{\psi^2 - B'}{A^n} = e$$

Genüge leisten kann. Da die erste derselben unmittelbar durch die Gleichung $\frac{\beta'^2 - A^n}{B'} = Bf^2$ erfüllt ist, so bleibt nur noch zu zeigen übrig, dafs man immer der zweiten

$$\frac{\psi^2 - B'}{A^n} = e$$

genügen könne.

Wir bezeichnen mit ϑ eine der Primzahlen, welche A^n teilen, und suchen die Zahl ψ von der Beschaffenheit, dafs $\frac{\psi^2 - B'}{\vartheta} = e$ ist. Wenn B' teilbar ist durch ϑ, so erhält man ψ gleich Null oder gleich einem Vielfachen von ϑ. Ist aber B' nicht durch ϑ teilbar, so sind zwei Fälle zu betrachten.

1) Ist ϑ ein Teiler von B, so wird es den Gleichungen

$$\alpha^2 - B = A^n A^{n-1} k^2, \quad \beta'^2 - A^n = BB'f^2$$

zufolge auch ein Teiler von α und β' sein. Man kann demnach folgende Reihe von ganzen Zahlen, die aus einander durch sehr einfache Substitutionen oder Rechnungen abgeleitet werden, aufstellen:

$$\frac{\beta^2 - A^{n-1}}{\vartheta} = e$$

$$\frac{k^2\beta^2 A^n - k^2 A^n A^{n-1}}{\vartheta^2} = e$$

$$\frac{k^2\beta^2 A^n + B}{\vartheta^2} = e$$

$$\frac{(\beta'^2 - BB'f^2)k^2\beta^2 + B}{\vartheta^2} = e$$

$$\frac{BB'f^2k^2\beta^2 - B}{\vartheta^2} = e$$

$$\frac{B'f^2k^2\beta^2 - 1}{\vartheta} = e$$

$$\frac{B'^2f^2k^2\beta^2 - B'}{\vartheta} = e.$$

Setzt man also:

$$\psi = B'fk\beta,$$

so erhält man:

$$\frac{\psi^2 - B'}{\vartheta} = e.$$

2) Ist ϑ kein Teiler von B, so ist es auch kein Teiler von α oder β' und man erhält nach und nach:

$$\frac{\alpha^2 - B}{\vartheta} = e$$

$$\frac{\alpha^2 f^2 B' - f^2 B B'}{\vartheta} = e$$

$$\frac{\alpha^2 f^2 B' - \beta'^2}{\vartheta} = e.$$

Da aber αf und ϑ prim zu einander sind, so kann man

$$\beta' = \psi \alpha f - m \vartheta$$

setzen, und dies giebt:

$$\frac{\psi^2 - B'}{\vartheta} = e.$$

Da dieselben Schlüsse bei allen Primfaktoren von A^n gelten, so folgt daraus, dafs man stets der Gleichung

$$\frac{\psi^2 - B'}{A^n} = e$$

genügen kann.

26.

Demnach wird die Gleichung $x^2 - By^2 = Az^2$ auflösbar sein, wenn man den beiden Bedingungen $\frac{\alpha^2 - B}{A} = e$, $\frac{\beta^2 - A}{B} = e$ und ferner bei der ersten transformierten Gleichung $x^2 - By^2 = A'z^2$ der dritten Bedingung $\frac{\beta'^2 - A'}{B} = e$ Genüge zu leisten imstande ist.

Diese dritte Bedingung würde, wie wir sogleich beweisen werden, überflüssig sein, im Falle die beiden Zahlen A und B zu einander prim wären. Der allgemeinere Satz kann indessen auf eine einfachere und gleichzeitig elegantere Weise dargestellt werden.

Wir bemerken zunächst, dafs sich jede unbestimmte Gleichung zweiten Grades zurückführen läfst auf die Form $ax^2 + by^2 = cz^2$, in welcher die Koefficienten positiv sind, keine zwei von ihnen einen gemeinsamen Teiler haben, und überdies von jedem quadratischen Faktor befreit sind. Das auf die Vorzeichen Bezügliche ist ohne weiteres ersichtlich, da jede aus drei Gröfsen gebildete Gleichung erfordert, dafs eine dieser Gröfsen gleich der Summe der beiden andern ist. Wenn ferner a einen quadratischen Faktor ϑ^2 enthielte, so könnte man $a = \vartheta^2 a'$, $x = \vartheta x'$ setzen, wodurch sich ax^2 in $a'x'^2$ verwandeln würde, und hierin hätte a' keinen quadratischen Faktor mehr. Wenn endlich zwei von den drei Koefficienten a, b, c z. B. a und b einen gemeinsamen Teiler ϑ hätten, so könnte man $a = a'\vartheta$, $b = b'\vartheta$, $c\vartheta = c'$, $z = z'\vartheta$ setzen. Dadurch würde sich die Gleichung $ax^2 + by^2 = cz^2$

in eine andere $a'x^2 + b'y^2 = c'z'^2$ verwandeln, in welcher a' und b' keinen gemeinschaftlichen Teiler mehr haben.

Nachdem dieses festgestellt ist, bringe man die Gleichung

$$ax^2 + by^2 = cz^2$$

auf die Form

$$\left(\frac{cz}{x}\right)^2 - bc\left(\frac{y}{x}\right)^2 = ac.$$

Diese kann man mit der Formel

$$x^2 - By^2 = Az^2$$

vergleichen, wodurch sich $B = bc$, $A = ac$ ergiebt. Man hat demnach zunächst die beiden Bedingungen zu erfüllen:

$$\frac{\alpha^2 - bc}{ac} = e, \quad \frac{\beta^2 - ac}{bc} = e.$$

Setzt man $\alpha = c\mu$, $\beta = c\nu$, so werden diese Bedingungen:

$$\frac{c\mu^2 - b}{a} = e, \quad \frac{c\nu^2 - a}{b} = e.$$

Um die dritte Bedingung $\frac{\beta'^2 - A'}{B} = e$ auszudrücken, bemerken wir, dafs $\alpha^2 - B = AA'k^2$ oder $c\mu^2 - b = aA'k^2$ ist, und da ak^2 keinen gemeinschaftlichen Teiler mit bc hat, so wird die letzte Bedingung erfüllt sein, wenn man

$$\frac{ak^2\beta'^2 - c\mu^2 + b}{bc} = e$$

hat. Damit nun der Zähler dieser Gröfse teilbar sei durch b, genügt es, wenn $ak^2\beta'^2 - c\mu^2$ durch b teilbar ist, oder es mufs, wenn man mit Berücksichtigung der zweiten Bedingung $c\nu^2$ an Stelle von a setzt, $k^2\beta'^2\nu^2 - \mu^2$ durch b teilbar sein, was immer möglich ist, wenn man β' der Gleichung $\frac{k\nu\beta' \pm \mu}{b} = e$ gemäfs bestimmt. Hieraus erkennt man, dafs, wenn A und B keinen gemeinsamen Teiler haben (oder wenn $c = 1$ ist), die dritte Bedingung eine Folge der beiden andern und somit gleichzeitig mit diesen erfüllt ist.

Haben sie jedoch einen gemeinsamen Teiler c, so bleibt noch die Bedingung

$$\frac{ak^2\beta'^2 + b}{c} = e, \text{ oder einfacher } \frac{a\lambda^2 + b}{c} = e$$

zu erfüllen. Wir haben also einen allgemeinen Satz, vermöge dessen man unmittelbar und ohne irgendwelche Transformation entscheiden kann, ob eine unbestimmte Gleichung zweiten Grades auflösbar ist oder nicht.

27.

Satz.

Ist die Gleichung $ax^2 + by^2 = cz^2$ gegeben, in welcher die einzelnen Koefficienten a, b, c keinen quadratischen Teiler und zu je zweien keinen gemeinschaftlichen Teiler haben, so wird diese Gleichung auflösbar sein, wenn sich drei ganze Zahlen λ, μ, ν von der Beschaffenheit finden lassen, dafs die drei Gröfsen

$$\frac{a\lambda^2 + b}{c}, \quad \frac{c\mu^2 - b}{a}, \quad \frac{c\nu^2 - a}{b}$$

ganze Zahlen werden. Sie wird dagegen unlösbar sein, wenn sich diese drei Bedingungen nicht gleichzeitig erfüllen lassen.

1. Bemerkung. Diese Bedingungen reducieren sich auf zwei, wenn eine der drei Zahlen a, b, c gleich 1 ist, und sie reducieren sich, wie in No. 22, auf eine einzige, wenn zwei dieser Zahlen gleich der Einheit sind.

2. Bemerkung. Man kann die drei Glieder der gegebenen Gleichung stets so anordnen, dafs a, b, c positiv sind; indessen ist dies keine unerläfsliche Bedingung, vielmehr würde der Satz auch richtig sein, wenn eines dieser Glieder negativ ist.

Jedoch darf man hieraus nicht schliefsen wollen, dafs eine Gleichung wie $x^2 + 5y^2 + 6z^2 = 0$ möglich sei, weil man den Bedingungen $\frac{\lambda^2 + 5}{6} = e$, $\frac{\mu^2 + 6}{5} = e$ genügen könne; man dürfte vielmehr nur schliefsen, dafs dieselbe auf die Form $x^2 + y^2 + z^2 = 0$ gebracht werden kann. Allgemein kann jede auflösbare Gleichung mittelst des im vorhergehenden Paragraphen angegebenen Verfahrens auf die Form

$$x^2 + y^2 - z^2 = 0$$

gebracht werden; jedoch reicht es hin, sie auf die Form zu bringen:

$$Ax^2 + y^2 - z^2 = 0,$$

deren Auflösung unmittelbar gegeben ist.

§ 5.

Entwicklung der Wurzel aus einer nichtquadratischen Zahl in einen Kettenbruch.

28.

Das in No. 1 auseinandergesetzte Verfahren zur Entwicklung einer beliebigen Zahlgröfse x in einen Kettenbruch kann mit grofser



Leichtigkeit auf die Quadratwurzeln der Zahlen oder allgemein auf Zahlgröfsen von der Form $\frac{\sqrt{A}+B}{C}$, wo A, B, C ganze Zahlen sind, angewandt werden.

Um den Gang der Rechnung recht klar hervortreten zu lassen, wollen wir erst ein specielles Beispiel nehmen.

Ist $A = 19$, so hat man x oder $\sqrt{19} = 4 + \frac{1}{x'}$, und hieraus $x' = \frac{1}{\sqrt{19}-4}$, oder, wenn man Zähler und Nenner des Bruches mit $\sqrt{19}+4$ multipliciert:

$$x' = \frac{\sqrt{19}+4}{3}.$$

Die gröfste in diesem Ausdrucke enthaltene ganze Zahl ist 2, so dafs man erhält:

$$x' = 2 + \frac{\sqrt{19}-2}{3}.$$

Nennt man diesen letzteren Teil $\frac{1}{x''}$, so ergiebt sich:

$$x'' = \frac{3}{\sqrt{19}-2} = \frac{\sqrt{19}+2}{5}.$$

Die hierin enthaltene ganze Zahl ist 1, der Rest $\frac{\sqrt{19}-3}{5}$. Diesen mufs man wieder umkehren, um den Wert von x''' zu erhalten u. s. w. Die Rechnung zur Entwicklung von $\sqrt{19}$ in einen Kettenbruch stellt sich also folgendermafsen:

$$\begin{aligned}
x &= \sqrt{19} &&= 4 + \frac{\sqrt{19}-4}{1}\\
x' &= \frac{1}{\sqrt{19}-4} = \frac{\sqrt{19}+4}{3} &&= 2 + \frac{\sqrt{19}-2}{3}\\
x'' &= \frac{3}{\sqrt{19}-2} = \frac{\sqrt{19}+2}{5} &&= 1 + \frac{\sqrt{19}-3}{5}\\
x''' &= \frac{5}{\sqrt{19}-3} = \frac{\sqrt{19}+3}{2} &&= 3 + \frac{\sqrt{19}-3}{2}\\
x^{IV} &= \frac{2}{\sqrt{19}-3} = \frac{\sqrt{19}+3}{5} &&= 1 + \frac{\sqrt{19}-2}{5}\\
x^{V} &= \frac{5}{\sqrt{19}-2} = \frac{\sqrt{19}+2}{3} &&= 2 + \frac{\sqrt{19}-4}{3}\\
x^{VI} &= \frac{3}{\sqrt{19}-4} = \frac{\sqrt{19}+4}{1} &&= 8 + \frac{\sqrt{19}-4}{1}\\
x^{VII} &= \frac{1}{\sqrt{19}-4} = \frac{\sqrt{19}+4}{3} &&= 2 + \text{u. s. w.}
\end{aligned}$$

Bis hierher gelangt, stöſst man auf einen Wert von x^{VII}, der demjenigen von x' gleich ist. Daraus folgt, daſs die bereits gefundenen Quotienten 2, 1, 3, 1, 2, 8 in derselben Reihenfolge wiederkehren werden, und daſs somit die Entwicklung von $\sqrt{19}$ in einen Kettenbruch die Quotienten:

4; 2, 1, 3, 1, 2, 8; 2, 1, 3, 1, 2, 8; 2, 1, 3, 1, 2, 8; u. s. w.

liefern wird. Man erkennt hieraus, daſs hinter dem ersten Gliede 4 die Periode 2, 1, 3, 1, 2, 8 stets in derselben Reihenfolge wiederkehrt und sich unendlich oft wiederholt.

29.

Ist jetzt A eine beliebige Zahl, a^2 die gröſste darin enthaltene Quadratzahl und b der Rest, so daſs man $A = a^2 + b$ hat, so ergiebt die **Entwicklung von $\sqrt{A}$ in einen Kettenbruch** zunächst:

$$x = \sqrt{A} = a + \frac{\sqrt{A} - a}{1}$$

$$x' = \frac{1}{\sqrt{A} - a} = \frac{\sqrt{A} + a}{b} = \text{u. s. w.}$$

Wir nehmen jetzt an, daſs man, wenn man diese Rechnung beliebig weit fortsetzt, zu einem vollständigen Quotienten $x^{(n)}$ oder $y = \frac{\sqrt{A} + J}{D}$ gelange. Ist dann μ die gröſste in y enthaltene ganze Zahl, so wird der Rest gleich $\frac{\sqrt{A} + J - \mu D}{D}$ sein. Nennt man diesen Rest $\frac{1}{y'}$, so erhält man:

$$y' = \frac{D}{\sqrt{A} + J - \mu D}.$$

Da aber ferner die Analogie der Formen erfordert, daſs man

$$y' = \frac{\sqrt{A} + J'}{D'}$$

habe, so ergiebt sich hieraus die folgende Gleichung zur Bestimmung von J' und D':

$$\frac{D}{\sqrt{A} + J - \mu D} = \frac{\sqrt{A} + J'}{D'}.$$

In dieser Gleichung hat man die rationalen Teile unter einander und die irrationalen Teile unter einander gleichzusetzen. Dies giebt:

$$J' = \mu D - J$$

$$D' = \frac{A - J'^2}{D}.$$

Dies ist das sehr einfache **Gesetz**, nach welchem sich aus einem beliebigen vollständigen Quotienten $\frac{\sqrt{A}+J}{D}$ der nächstfolgende vollständige Quotient $\frac{\sqrt{A}+J'}{D'}$ ableitet. Dabei ist nicht zu befürchten, daſs die Zahlen J' und D' Brüche seien. Denn setzt man den Wert von J' in den von D' ein, so erhält man:

$$D' = \frac{A-(\mu D-J)^2}{D} = \frac{A-J^2}{D} + 2\mu J - \mu^2 D.$$

Da nun $A - J'^2 = D'D$ ist, so ergiebt sich in analoger Weise, wenn man den $\frac{\sqrt{A}+J}{D}$ vorhergehenden vollständigen Quotienten mit $\frac{\sqrt{A}+J^0}{D^0}$ bezeichnet, $A - J^2 = DD^0$, mithin:

$$D' = D^0 + 2\mu J - \mu^2 D.$$

Daraus ist ersichtlich, daſs, weil die Zahlen D und J in den beiden ersten vollständigen Quotienten $\frac{\sqrt{A}+0}{1}$, $\frac{\sqrt{A}+a}{b}$ ganze Zahlen sind, dieselben notwendigerweise auch bei allen andern bis ins Unendliche hin ganze Zahlen sein werden.

Der soeben gefundene Wert für D' läſst sich auch auf die Form bringen:

$$D' = D^0 + \mu(J - J').$$

Mithin ergiebt sich aus den beiden aufeinanderfolgenden vollständigen Quotienten

$$\frac{\sqrt{A}+J^0}{D^0} = \mu^0 +$$

$$\frac{\sqrt{A}+J}{D} = \mu +$$

der nächstfolgende vollständige Quotient $\frac{\sqrt{A}+J'}{D'}$ mit Hülfe der Formeln:

$$J' = \mu D - J$$
$$D' = D^0 + \mu(J - J').$$

Hierdurch ist das **Fortschreitungsgesetz** auf die einfachste Weise dargestellt.

30.

Nehmen wir jetzt an, daſs $\frac{p^0}{q^0}$, $\frac{p}{q}$ zwei aufeinanderfolgende Näherungsbrüche von $\sqrt{A}$ seien und $\frac{\sqrt{A}+J}{D}$ der dem Bruche $\frac{p}{q}$

entsprechende vollständige Quotient, so hat man dem bekannten Prinzipe zufolge:

$$\sqrt{A} = \frac{p\left(\frac{\sqrt{A}+J}{D}\right)+p^0}{q\left(\frac{\sqrt{A}+J}{D}\right)+q^0} = \frac{p\sqrt{A}+pJ+p^0D}{q\sqrt{A}+qJ+q^0D}.$$

Hieraus folgert man die beiden Gleichungen:

$$pJ + p^0D = qA$$
$$qJ + q^0D = p,$$

und diese geben:

$$(pq^0 - p^0q)J = qq^0A - pp^0$$
$$(pq^0 - p^0q)D = p^2 - Aq^2.$$

Nach der Eigenschaft der Kettenbrüche (No. 6) ist aber:

$$pq^0 - p^0q = +1, \text{ wenn } \frac{p}{q} > \sqrt{A}$$

$$pq^0 - p^0q = -1, \text{ wenn } \frac{p}{q} < \sqrt{A}.$$

Daraus ersieht man, dafs $pq^0 - p^0q$ stets dasselbe Vorzeichen hat, wie $p^2 - Aq^2$, und dafs somit D stets positiv ist. Ferner zeigen diese Werte unmittelbar, dafs D und J stets ganze Zahlen sind; wir behaupten aber noch weiter, dafs auch J stets positiv ist. Denn einerseits giebt die Gleichung $qJ + q^0D = p$ die folgende:

$$\frac{q^0}{q} = \left(\frac{p}{q} - J\right) : D,$$

und da $q^0 < q$ ist, so mufs sein:

$$D > \frac{p}{q} - J \text{ oder } D > \sqrt{A} - J;$$

andrerseits hat man:

$$\frac{\sqrt{A}+J}{D} > \mu, \text{ also } D < \sqrt{A} + J.$$

Diese beiden Bedingungen würden aber mit einander unvereinbar sein, wenn J negativ wäre.

Nachdem wir dieses festgestellt haben, können wir auch leicht **die Grenzen** finden, welche J und D nicht übersteigen dürfen. Die Gleichung $A - J^2 = DD^0$ ergiebt $J < \sqrt{A}$. Mithin könnte J die gröfste in $\sqrt{A}$ enthaltene ganze Zahl a nicht übersteigen. Da ferner $J + J' = \mu D$ ist, so folgt, dafs $2a$ die Grenze von D und zugleich auch die des Quotienten μ ist.

Da jedoch der Kettenbruch, welcher den Wert einer irrationalen Zahlgröfse darstellt, sich ins Unendliche erstrecken mufs, und da es

nur eine bestimmte Anzahl verschiedener Werte sowohl für J als für D geben kann, so mufs notwendig derselbe Wert von J unendlich oftmal mit demselben Werte von D zusammentreffen. Sobald man aber für den vollständigen Quotienten $\frac{\sqrt{A}+J}{D}$ einen bereits gefundenen Wert noch einmal findet, so ist klar, dafs auch die folgenden Quotienten des Kettenbruches dieselben sein und in derselben Reihenfolge vorkommen müssen, wie die bereits erhaltenen. Mithin wird der Kettenbruch, welcher $\sqrt{A}$ darstellt, (wenigstens nach einigen Gliedern) aus einer beständigen, sich bis Unendliche hin wiederholenden Periode bestehen, wie wir dies bereits bei einem speciellen Falle (No. 28) gesehen haben.

31.

Es handelt sich nunmehr darum, genau **die Stelle** zu bestimmen, **an welcher die Periode beginnt.** Wir werden annehmen, dafs $\mu, \mu', \mu'', \ldots \omega$ diese Periode ist, und werden wie gewöhnlich die Reihe der Quotienten und die Reihe der ihnen bis zum Beginn der zweiten Periode entsprechenden Näherungsbrüche folgendermafsen bezeichnen:

Quotienten: $a,\ \alpha,\ \beta,\ \gamma \ldots\ \lambda,\ \mu,\ \mu',\ \mu'', \ldots\ \omega,\ \mu,\ \mu',\ \mu'', \ldots \omega$ u.s.w.

Näherungsbrüche: $\frac{1}{0},\ \frac{a}{1},\ \ldots\ldots \frac{p^0}{q^0},\ \frac{p}{q},\ \ldots\ldots \frac{p^0{}_I}{q^0{}_I},\ \frac{p_I}{q_I} \ldots$

Sind dann gleichzeitig die entsprechenden Werte des vollständigen Quotienten:

$$\frac{\sqrt{A}}{1},\ \frac{\sqrt{A}+a}{b},\ \ldots \frac{\sqrt{A}+J^0}{D^0},\ \frac{\sqrt{A}+J}{D},\ \ldots \frac{\sqrt{A}+J^0{}_I}{D^0{}_I},\ \frac{\sqrt{A}+J}{D},\ \ldots,$$

so erhält man zunächst dem Bewiesenen zufolge:

$$A - J^2 = DD^0,$$

und

$$A - J^2 = DD^0{}_I.$$

Dies giebt:

$$D^0{}_I = D^0.$$

Ferner hat man:

$$J = \lambda D^0 - J^0,$$

und

$$J = \omega D^0{}_I - J^0{}_I,$$

und hieraus ergiebt sich:

$$\frac{J^0 - J^0{}_I}{D^0} = \lambda - \omega.$$

Andrerseits aber folgt aus der Gleichung $qJ + q^0 D = p$:

$$J = \frac{p}{q} - \frac{q^0 D}{q}.$$

Da nun $\frac{p}{q}$ ein Näherungswert von $\sqrt{A}$ ist, so mufs sein:

$$\frac{p}{q} = a + \text{einem Bruch } \frac{r}{q}.$$

Mithin:

$$a - J = \frac{q^0 D - r}{q}.$$

Wegen $q^0 < q$ erhält man also:

$$a - J < D.$$

In analoger Weise ist:

$$a - J^0 < D^0$$
$$a - J^0{}_I < D^0{}_I,$$

daher umsomehr:

$$J^0 - J^0{}_I < D^0.$$

Da wir aber bereits $\frac{J^0 - J^0{}_I}{D^0}$ gleich der ganzen Zahl $\lambda - \omega$ gefunden hatten, so mufs diese ganze Zahl notwendig Null sein. Man erhält also:

$$J^0 = J^0{}_I \text{ und } \lambda = \omega.$$

Ebenso beweist man, dafs der Quotient, welcher λ vorhergeht, gleich demjenigen ist, welcher ω vorhergeht, und so fort bis zum Quotienten α, so dafs also α derjenige Quotient ist, welcher zuerst wiederkehrt und die Periode beginnen mufs.

32.

Hiernach kann man die Reihe der Quotienten und die Reihe der ihnen bei der Entwicklung von $\sqrt{A}$ entsprechenden Näherungsbrüche in folgender Weise darstellen:

Quotienten:

$a;\ \alpha,\ \beta,\ \ldots\ \lambda,\ \mu;\ \ \alpha,\ \beta,\ \ldots\ \lambda,\ \mu;\ \ \alpha,\ \beta,\ \ldots\ \lambda,\ \mu,$ u. s. w.

Näherungsbrüche:

$$\frac{1}{0},\ \frac{a}{1},\ \ldots\ldots \frac{p^0}{q^0},\ \frac{p}{q};\ \frac{p'}{q'},\ \ldots\ldots \frac{p^0{}_I}{q^0{}_I},\ \frac{p_I}{q_I},\ \frac{p'_I}{q'_I},\ \ldots.$$

Bei dieser Aufstellung ist $\frac{p}{q}$ der Näherungsbruch, welcher dem letzten Quotienten μ der ersten Periode $\alpha, \beta, \ldots \lambda, \mu$ entspricht. Ist z der entsprechende vollständige Quotient, so hat man $z - \mu = \sqrt{A} - a$ oder $z = \mu - a + \sqrt{A}$, und hieraus ergiebt sich, dem gewöhnlichen Prinzipe zufolge:

$$\sqrt{A} = \frac{pz + p^0}{qz + q^0} = \frac{p\sqrt{A} + p(\mu - a) + p^0}{q\sqrt{A} + q(\mu - a) + q^0}.$$

Diese Gleichung liefert die beiden folgenden:

$$p(\mu - a) + p^0 = Aq$$
$$q(\mu - a) + q^0 = p.$$

Die zweite Gleichung giebt:

$$\mu - a + \frac{q_0}{q} = \frac{p}{q},$$

und hieraus folgt, dafs $\mu - a$ die gröfste in $\frac{p}{q}$ enthaltene ganze Zahl ist. Diese ganze Zahl ist gleich a, so dafs man hat:

$$\mu - a = a, \text{ oder } \mu = 2a.$$

Zu gleicher Zeit ergiebt sich, da $q^0 = p - aq$ ist, dafs die Reihe der Quotienten $\alpha, \beta, \ldots \vartheta, \lambda$, welche μ vorhergehen, symmetrisch ist (No. 11); denn es ist $\frac{p - aq}{q}$ einer der Näherungsbrüche von $\sqrt{A} - a$, einer Gröfse, die gleich ist dem Kettenbruche:

$$\frac{1}{\alpha} + \frac{1}{\beta} + \cdots$$

Diesem Näherungsbruche geht unmittelbar der folgende $\frac{p^0 - aq^0}{q^0}$ vorher; da man nun $q^0 = p - aq$ hat, so mufs die Periode $\alpha, \beta, \ldots \vartheta, \lambda$ identisch sein mit der zu ihr inversen $\lambda, \vartheta, \ldots \beta, \alpha$. Aus allen diesen Bemerkungen folgt, dafs die Quotienten, welche aus der Entwicklung von $\sqrt{A}$ entspringen, nach folgendem Gesetze fortschreiten:

$$a;\ \alpha, \beta, \gamma, \ldots \gamma, \beta, \alpha, 2a;\ \alpha, \beta, \gamma, \ldots \gamma, \beta, \alpha, 2a; \text{ u. s. w.},$$

ein Gesetz, welches noch regelmäfsiger sein würde, wenn der erste Quotient $2a$ oder 0 wäre, d. h. wenn es sich um die Entwicklung von $\sqrt{A} \pm a$ handelte.

33.

Es ist wichtig, zu bemerken, dafs jeder Näherungsbruch $\frac{p}{q}$, welcher dem Quotienten $2a$ in irgend einer Periode entspricht, von solcher Beschaffenheit ist, dafs die Gleichung gilt:

$$p^2 - Aq^2 = \pm 1.$$

Denn ist der Quotient $\mu = 2a$, so giebt die Gleichung $J^0 + J = D\mu$, in welcher J und J^0 a nicht übersteigen können (No. 30), notwendig:

$$J = J^0 = a, \quad D = 1.$$

Mithin geht die Gleichung

$$(pq^0 - p^0 q) D = p^2 - Aq^2$$

über in:

$$p^2 - Aq^2 = \pm 1,$$

wobei das Zeichen $+$ gilt, wenn $\frac{p}{q} > \sqrt{A}$ ist, das Zeichen $-$ im entgegengesetzten Falle.

Da der Quotient $2a$ notwendig in der Entwicklung von $\sqrt{A}$ vorkommt, so folgt daraus, daſs die Gleichung $x^2 - Ay^2 = \pm 1$ jederzeit auflösbar ist (wenigstens mit dem Zeichen $+$), welches auch die Zahl A sein möge, vorausgesetzt, daſs sie kein vollständiges Quadrat ist. Zugleich sieht man, daſs es unendlich viele Lösungen dieser Gleichung giebt, da der Quotient $2a$ sich unendlich oftmal in den aufeinanderfolgenden Perioden wiederholt.

Wenn übrigens die Anzahl der Glieder der Periode $\alpha, \beta, \ldots \beta, \alpha, 2a$ gerade ist, so werden alle Brüche, welche dem Quotienten $2a$ in den verschiedenen Perioden entsprechen, gröſser als $\sqrt{A}$ sein, und es werden somit in diesem Falle die Brüche der Gleichung

$$x^2 - Ay^2 = +1$$

genügen. Wenn dagegen die Anzahl der Glieder der Periode ungerade ist, so wird der erste dem Quotienten $2a$ entsprechende Bruch kleiner als $\sqrt{A}$, der zweite gröſser sein und so abwechselnd weiter. In diesem Falle wird daher die Gleichung $x^2 - Ay^2 = -1$ ebenso gut auflösbar sein, wie die Gleichung $x^2 - Ay^2 = +1$; erstere durch die Näherungsbrüche von ungerader, letztere durch die von gerader Ordnung.

§ 6.

Auflösung der unbestimmten Gleichung $x^2 - Ay^2 = \pm D$ in ganzen Zahlen für den Fall, daſs $D < \sqrt{A}$ ist.

34.

Im vorhergehenden Paragraphen haben wir gezeigt, daſs die Gleichung $x^2 - Ay^2 = +1$ immer auf unendlich viele Arten auflösbar ist, wie beschaffen auch A sein möge, wofern es nur kein vollständiges Quadrat ist. Dagegen ist die Gleichung $x^2 - Ay^2 = -1$ nur in gewissen besonderen Fällen auflösbar, und da die Auflösung, wenn sie möglich ist, sich unter den Näherungsbrüchen von $\sqrt{A}$ vorfinden muſs, so ist die notwendige und zugleich hinreichende Bedingung für die Möglichkeit dieser Auflösung, daſs die Periode der

Quotienten, welche durch die Entwicklung von $\sqrt{A}$ gegeben wird, aus einer ungeraden Anzahl von Gliedern bestehe.

Die Auflösungen einer jeden der beiden Gleichungen erhält man unmittelbar aus den Näherungsbrüchen von $\sqrt{A}$, nämlich aus denjenigen, welche dem Quotienten $2a$ entsprechen (wo a die gröfste in $\sqrt{A}$ enthaltene ganze Zahl ist). Solcher giebt es unendlich viele, da dieser Quotient, ebenso wie die ihn enthaltenden Perioden, sich unendlich oft wiederholt. Der Zähler jedes Bruches ist ein Wert von x, sein Nenner der zugehörige Wert von y.

Wir werden weiter unten zeigen, wie man den allgemeinen Ausdruck der verschiedenen Brüche, welche einem und demselben, in den aufeinanderfolgenden Perioden an derselben Stelle befindlichen Quotienten entsprechen, a priori finden kann. Für den gegenwärtigen Fall genügt es, das Resultat, das man übrigens unmittelbar bewahrheiten kann, kennen zu lernen.

Es sei $\frac{p}{q}$ der erste und einfachste der Näherungsbrüche, welche einem und demselben Quotienten $2a$ entsprechen. Hat man dann:

$$p^2 - Aq^2 = +1,$$

oder ist die **Anzahl der Glieder der Periode gerade**, so wird nur allein die Gleichung $x^2 - Ay^2 = +1$ auflösbar sein, wie wir bereits angegeben haben. Wenn man alsdann die allgemeine Auflösung haben will, braucht man nur $p + q\sqrt{A}$ auf irgend eine Potenz m zu erheben und das Resultat gleich $x + y\sqrt{A}$ zu setzen. Ist nämlich:

$$(p + q\sqrt{A})^m = x + y\sqrt{A},$$

wo x und y rationale Zahlen sind, so hat man zugleich:

$$(p - q\sqrt{A})^m = x - y\sqrt{A}.$$

Multipliciert man beide Gleichungen mit einander, so wird ihr Produkt:

$$x^2 - Ay^2 = (p^2 - Aq^2)^m = 1^m = 1.$$

Mithin genügen die gefundenen Werte für x und y wirklich der Gleichung $x^2 - Ay^2 = 1$, welches auch der Exponent m sein möge. Man kann auch die Werte von x und y mittelst der Formeln:

$$x = \frac{(p + q\sqrt{A})^m + (p - q\sqrt{A})^m}{2}$$

$$y = \frac{(p + q\sqrt{A})^m - (p - q\sqrt{A})^m}{2\sqrt{A}},$$

welche immer ganze Zahlen für x und y ergeben, besonders darstellen.

35.

Ist zweitens:

$$p^2 - Aq^2 = -1,$$

oder ist die **Anzahl der Glieder der Periode ungerade**, so ist ersichtlich, dafs man immer gleichzeitig den beiden Gleichungen:

$$x^2 - Ay^2 = +1, \quad x^2 - Ay^2 = -1$$

genügen kann, und zwar der ersteren mittelst gerader Potenzen von $p + q\sqrt{A}$, der zweiten mittelst ungerader Potenzen desselben Binoms. Denn setzt man:

$$(p + q\sqrt{A})^{2k} = x + y\sqrt{A},$$

so erhält man:

$$x^2 - Ay^2 = (-1)^{2k} = +1;$$

und setzt man:

$$(p + q\sqrt{A})^{2k+1} = x + y\sqrt{A},$$

so wird:

$$x^2 - Ay^2 = (-1)^{2k+1} = -1.$$

Ist z. B. $A = 13$, so findet man $\frac{p}{q} = \frac{18}{5}$ und $p^2 - 13q^2 = -1$. Setzt man also:

$$(18 + 5\sqrt{13})^{2k} = x + y\sqrt{13},$$

so genügt man der Gleichung $x^2 - 13y^2 = 1$, und setzt man:

$$(18 + 5\sqrt{13})^{2k+1} = x + y\sqrt{13},$$

so genügt man der Gleichung $x^2 - 13y^2 = -1$.

Die kleinsten Zahlen, welche der Gleichung $x^2 - 13y^2 = 1$ Genüge leisten, sind demnach $x = 649$, $y = 180$; denn man hat $(18 + 5\sqrt{13})^2 = 649 + 180\sqrt{13}$.

Zuweilen sind die einfachsten Zahlen, welche einer gegebenen Gleichung $x^2 - Ay^2 = \pm 1$ genügen, weit beträchtlicher. Z. B. ist die einfachste Lösung der Gleichung $x^2 - 211y^2 = 1$:

$$x = 278354373650$$
$$y = 19162705353,$$

und die einfachste Lösung der Gleichung $x^2 - 991y^2 = 1$ ist:

$$x = 379516\,400906\,811930\,638014\,896080$$
$$y = 12055\,735790\,331359\,447442\,538767.$$

Hieraus ersieht man, wie notwendig es für die Aufsuchung dieser Zahlen ist, eine sichere und unfehlbare Methode, wie es die entwickelte ist, zu haben. Denn man würde sich sehr irren, wenn man, nach-

dem man vergeblich die Auflösung mittelst mäſsig groſser Zahlen versucht hätte, schlieſsen wollte, daſs sie überhaupt für keine Zahlen möglich sei.

36.

Fermat ist der erste, der die Auflösung der Gleichung

$$x^2 - Ay^2 = 1$$

gekannt zu haben scheint; wenigstens legte er diese Aufgabe gleichsam als Herausforderung den englischen Mathematikern vor. Lord Brounker gab eine Auflösung derselben, welche man in den Werken von Wallis findet und die fast wörtlich in den zweiten Teil von Euler's Algebra aufgenommen ist. Aber einerseits hat Fermat nichts über seine eigene Auflösung veröffentlicht, andererseits zeigt die, wenn auch sehr geistreiche, Methode der englischen Mathematiker doch nicht in bestimmer Weise, daſs die Aufgabe immer lösbar sei. Es blieb daher noch zu beweisen übrig, daſs die Gleichung $x^2 - Ay^2 = 1$ stets in ganzen Zahlen auflösbar ist. Dies hat Lagrange in ebenso eleganter wie strenger Weise in den „Gemischten Abhandlungen der Turiner Akademie“ Band IV und sodann in den Abhandlungen der Berliner Akademie vom Jahre 1767 gethan. Dieser Beweis, sowie die ihm beigegebene Methode der Auflösung müssen als einer der wichtigsten Schritte, welche bis heute in der unbestimmten Analysis gemacht worden sind, betrachtet werden. In der That ist die Gleichung $x^2 - Ay^2 = 1$ nicht allein an und für sich interessant; sie ist auch bei der Auflösung aller unbestimmten Gleichungen zweiten Grades erforderlich, wo sie dazu dient, unendlich viele Auflösungen zu finden, wenn man eine einzige solche kennt.

Am Ende dieses Werkes wird man eine Tafel, No. X, finden, welche unter der Form von Brüchen die einfachsten Lösungen der Gleichung $m^2 - An^2 = \pm 1$ für jede Zahl A von 2 bis zu 1003 enthält, welche nicht Quadratzahl ist.

Der bloſse Anblick der Ziffern, mit denen die Zahlen m und n endigen, läſst erkennen, ob sie der Gleichung

$$m^2 - An^2 = +1$$

oder der Gleichung

$$m^2 - An^2 = -1$$

genügen. Erfüllen sie diese letztere, so muſs man, um die kleinsten Zahlen p und q, welche der Gleichung $x^2 - Ay^2 = +1$ genügen, zu erhalten, $(m + n\sqrt{A})^2 = p + q\sqrt{A}$ setzen. Man erhält alsdann $p = 2m^2 + 1$, $q = 2mn$.



37.

Wir gehen nunmehr zur **Auflösung** der gegebenen Gleichung

$$x^2 - Ay^2 = \pm D$$

über. Wir haben Nr. 10 gesehen, dafs, wenn $D < \sqrt{A}$ ist, wie wir es voraussetzen, der Bruch $\frac{x}{y}$ einer der Näherungsbrüche von $\sqrt{A}$ sein mufs. Man wird daher $\sqrt{A}$ in einen Kettenbruch entwickeln und die aufeinanderfolgenden Werte der vollständigen Quotienten $\frac{\sqrt{A} + J}{D}$ berechnen müssen. Findet sich unter diesen vollständigen Quotienten einer, dessen Nenner D gleich der rechten Seite der gegebenen Gleichung ist, so folgt daraus eine Lösung entweder der Gleichung $x^2 - Ay^2 = + D$, oder der Gleichung $x^2 - Ay^2 = - D$. Dazu mufs man den Näherungsbruch $\frac{p}{q}$ berechnen, welcher dem betreffenden vollständigen Quotienten entspricht. Ist dieser Bruch von ungerader Ordnung (wobei $\frac{1}{0}$ als der erste gerechnet wird), so wird er gröfser als $\sqrt{A}$ und mithin $p^2 - Aq^2 = + D$ sein. Ist er aber von gerader Ordnung, so wird man $p^2 - Aq^2 = - D$ haben.

Dieselbe Zahl D kann in einer und derselben Periode mehrere Male vorkommen, und zwar wird sie, da die Periode symmetrisch ist, sich stets mindestens zweimal vorfinden (den Fall ausgenommen, wo der Quotient, welchem $\frac{p}{q}$ entspricht, das mittelste Glied der Periode ist, wenn man von ihrem letzten Gliede $2a$ absieht). Man erhält alsdann ebenso viele Lösungen entweder der Gleichung $x^2 - Ay^2 = + D$ oder der Gleichung $x^2 - Ay^2 = - D$, und dieses wird bei allen andern Perioden ebenfalls stattfinden.

Findet man die Zahl D nicht unter den Nennern der vollständigen Quotienten in der ersten Periode, so kann man sicher sein, dafs weder die Gleichung $x^2 - Ay^2 = + D$, noch die Gleichung $x^2 - Ay^2 = - D$ in ganzen Zahlen auflösbar ist.

38.

Hat man aber eine oder mehrere Lösungen, welche in der Weise, wie wir es eben auseinandergesetzt haben, durch die erste Periode der Quotienten gegeben werden, so kann man aus jeder

von diesen ersten Lösungen unmittelbar eine **allgemeine Formel** ableiten, welche eine **unendliche Menge anderer** von dieser ersten abhängender Lösungen enthält.

Es sei $\frac{p}{q}$ der Näherungsbruch, für welchen $p^2 - Aq^2 = D$ ist, und zu gleicher Zeit seien t und u irgendwelche der Gleichung $t^2 - Au^2 = 1$ genügende Zahlen. Multipliciert man beide Gleichungen mit einander, so kann man das Produkt auf die Form bringen:

$$(pt \pm Aqu)^2 - A(pu \pm qt)^2 = D,$$

so dafs die allgemeine Auflösung der Gleichung $x^2 - Ay^2 = D$ gegeben wird durch die Formeln:

$$x = pt \pm Aqu$$
$$y = pu \pm qt.$$

Was die Werte von t und u anlangt, so haben wir bereits gezeigt, dafs, wenn m und n die kleinsten, der Gleichung $m^2 - An^2 = 1$ genügenden Zahlen sind und man für k eine beliebige ganze Zahl nimmt, man hat:

$$(m + n\sqrt{A})^k = t + u\sqrt{A}.$$

Man sieht daher, dafs man, wenn man von den verschiedenen ursprünglichen Lösungen, welche in der ersten Periode enthalten sind, ausgeht, ebensoviele allgemeine Formeln erhalten wird, deren jede unendlichviele Lösungen der gegebenen Gleichung in sich begreift.

Übrigens gelten die Werte, welche wir soeben für x und y gegeben haben, in gleicher Weise, mag D positiv oder mag es negativ sein. Sie setzen nur voraus, dafs D in der speciellen Gleichung $p^2 - Aq^2 = D$ dasselbe Zeichen habe wie in der allgemeinen Gleichung $x^2 - Ay^2 = D$; sie setzen ferner voraus, dafs $m^2 - An^2 = +1$ sei.

Wäre $m^2 - An^2 = -1$, so würden die Formeln

$$x = pt \pm Aqu$$
$$y = pu \pm qt$$

gleichzeitig die Auflösung der Gleichung $x^2 - Ay^2 = +D$ und diejenige der Gleichung $x^2 - Ay^2 = -D$ geben, nämlich die der ersteren, wenn man $(m + n\sqrt{A})^{2k} = t + u\sqrt{A}$, die der letzteren, wenn man $(m + n\sqrt{A})^{2k+1} = t + u\sqrt{A}$ setzte.

39.

Wenn man, sei es aus der eben erwähnten Tafel, sei es auf irgend eine andere Weise, den einfachsten Bruch $\frac{m}{n}$ kennt, welcher

der Gleichung $m^2 - An^2 = \pm 1$ genügt, so wird die einfache Entwicklung von $\frac{m}{n}$ in einen Kettenbruch die Periode der Quotienten ergeben, welche aus der Entwicklung von $\sqrt{A}$ hervorgehen würden. Demnach kann man, ohne die diesen ganzzahligen Quotienten entsprechenden vollständigen Quotienten $\frac{\sqrt{A}+J}{D}$ zu kennen und mithin ohne ihre Nenner zu wissen, dennoch leicht diejenigen herausfinden, welche einem gegebenen Werte von N entsprechen. Diese Quotienten sind ziemlich nahe gleich $\frac{2a}{D}$, wo a die gröfste in $\sqrt{A}$ enthaltene ganze Zahl bedeutet. In der That ergiebt sich, da (nach No. 30)

$$J = \frac{p - q^0 D}{q}$$

ist,

$$\frac{\sqrt{A}+J}{D} = \frac{\frac{p}{q} + \sqrt{A}}{D} - \frac{q^0}{q}.$$

Mithin ist die gröfste in $\frac{\sqrt{A}+J}{D}$ enthaltene ganze Zahl μ sehr nahe gleich der in $\frac{2a}{D}$ enthaltenen gröfsten ganzen Zahl.

40.

Soll z. B. die Gleichung:

$$x^2 - 61y^2 = 5$$

aufgelöst werden, so entwickele man den Bruch $\frac{29718}{3805}$, dessen Zähler und Nenner der Gleichung $m^2 - 61n^2 = -1$ genügen, in einen Kettenbruch. Die Quotienten und Näherungsbrüche findet man folgendermafsen:

Quotienten:

7, 1, 4, 3, 1, 2, 2, 1, 3, 4, 1, ...

Näherungsbrüche:

$$\frac{1}{0}, \frac{7}{1}, \frac{8}{1}, \frac{39}{5}, \frac{125}{16}, \frac{164}{21}, \frac{453}{58}, \frac{1070}{137}, \frac{1523}{195}, \frac{5639}{722}, \frac{24079}{3083}, \frac{29718}{3805}.$$

Die gröfste in $\sqrt{61}$ enthaltene ganze Zahl ist 7 und $\frac{2 \cdot 7}{5} = 2 + \cdots$ Sucht man also 2 unter den Quotienten, so findet man die beiden entsprechenden Brüche $\frac{164}{21}$ und $\frac{453}{58}$, deren erster $p^2 - 61q^2 = -5$, deren letzterer $p^2 - 61q^2 = 5$ giebt. Mithin wird die gegebene Gleichung $x^2 - 61y^2 = 5$ mittelst der Formeln aufgelöst werden:

$$x = 453t \pm 3538u$$
$$y = 453u \pm 58t$$
$$t + u\sqrt{61} = (29718 + 3805\sqrt{61})^{2k},$$

und ferner ebenfalls durch die folgenden Formeln, welche mit Hülfe des ersten Näherungsbruches $\frac{164}{21}$ berechnet sind:

$$x = 164t \pm 1281u$$
$$y = 164u \pm 21t$$
$$t + u\sqrt{61} = (29718 + 3805\sqrt{61})^{2k+1}.$$

Auf dieselbe Weise würde man die Gleichung $x^2 - 61y^2 = -5$ lösen, und man erkennt, warum die beiden für $\frac{p}{q}$ gefundenen Werte, obgleich sie für D zwei Werte mit verschiedenen Zeichen geben, dennoch zur Auflösung einer und derselben Gleichung dienen. Der Grund liegt darin, dafs der Wert von $\frac{m}{n}$ ein solcher ist, für welchen $m^2 - 61n^2 = -1$ ist. Denn in allen ähnlichen Fällen giebt eine Auflösung der Gleichung $x^2 - Ay^2 = D$ immer eine Auflösung der Gleichung $x^2 - Ay^2 = -D$ und umgekehrt.

41.

Wir bemerken noch, dafs, wenn D, obwohl stets kleiner als $\sqrt{A}$, einen quadratischen Faktor ϑ^2 hätte, so dafs $D = \vartheta^2 D'$ wäre, man alsdann aufser den Lösungen, die wir nach der vorhergehenden Methode gefunden haben, und bei denen x und y stets prim zu einander sind, noch andere erhalten könnte, bei denen x und y den gemeinsamen Teiler ϑ hätten. Hätte man nämlich auf andere Weise gefunden, dafs die Lösung der Gleichung $x'^2 - Ay'^2 = D'$ möglich sei, so ist klar, dafs man daraus $x = \vartheta x'$, $y = \vartheta y'$ erhalten würde. Auf diese Weise wird es so viele neue Auflösungsformeln geben können, als es Arten giebt, die Zahl D durch eine Quadratzahl zu teilen.

§ 7.

Sätze über die Möglichkeit der Gleichungen von der Form: $Mx^2 - Ny^2 = \pm 1$ oder ± 2.

42.

Wir setzen voraus, dafs A eine Primzahl und p und q die kleinsten Zahlen (1 und 0 ausgeschlossen) seien, welche der Gleichung

$$p^2 - Aq^2 = 1$$

genügen. Diese Gleichung läſst sich auf die Form bringen:

$$p^2 - 1 = Aq^2 \text{ oder } (p+1)(p-1) = Aq^2.$$

Da nun A eine Primzahl ist, so kann diese Gleichung, wenn man $q = fgh$ setzt, nur auf folgende zwei Arten zerlegt werden:

$$\left.\begin{aligned} p+1 &= fg^2A \\ p-1 &= fh^2 \end{aligned}\right\} \qquad \begin{aligned} p+1 &= fg^2 \\ p-1 &= fh^2A. \end{aligned}$$

Es muſs demnach eine der beiden nachstehenden Gleichungen stattfinden:

$$-\frac{2}{f} = h^2 - Ag^2, \quad \frac{2}{f} = g^2 - Ah^2.$$

Aus diesen letzteren erkennt man, daſs f nur 1 oder 2 sein kann, so daſs man die vier Kombinationen erhält:

$$(1) \quad -1 = h^2 - Ag^2, \qquad (3) \quad 1 = g^2 - Ah^2$$

$$(2) \quad -2 = h^2 - Ag^2, \qquad (4) \quad 2 = g^2 - Ah^2.$$

Von diesen ist jedoch die Kombination (3) auszuschlieſsen, da aus ihr sich ergeben würde, daſs p und q nicht die kleinsten der Gleichung $p^2 - Aq^2 = 1$ genügenden Zahlen seien. Es bleiben daher nur noch die drei andern Kombinationen zu diskutieren übrig. Dazu müssen wir nach einander die verschiedenen Formen betrachten, welche A mit Bezug auf die Vielfachen von 4 oder 8 annehmen kann.

43.

Ist erstens A von der Form $4n + 1$, so muſs, wenn in den Gleichungen (2) und (4) die eine der beiden Zahlen g und h gerade ist, auch die andere gerade sein. Alsdann aber würde die rechte Seite durch 4 teilbar sein, während die linke ± 2 ist, was mit einander nicht im Einklang steht. Nimmt man sodann die beiden Zahlen g und h als ungerade an, so werden ihre Quadrate g^2 und h^2 von der Form $8n + 1$, und es wird die rechte Seite ebenfalls durch 4 teilbar sein. Mithin ist die Gleichung (1) die einzige, welche stattfinden kann; sie findet demnach notwendig statt, und daraus ergiebt sich folgender sehr bemerkenswerte **Satz:**

Ist A eine Primzahl von der Form $4n + 1$, so ist die Gleichung

$$x^2 - Ay^2 = -1$$

stets möglich.

Diese Eigenschaft findet für die Primzahlen von der Form $4n + 1$ ausschlieſslich statt. Denn wenn A von der Form $4n + 3$ wäre, so



erkennt man leicht, dafs, wenn x und y gerade oder ungerade Werte beigelegt werden, $x^2 - Ay^2$ immer von einer der Formen $4n$, $4n + 1$, $4n + 2$ sein würde, unter denen -1 nicht enthalten ist.

Man bemerke noch, dafs, wenn A eine Primzahl von der Form $4n + 1$ ist, jede Zahl, welche durch die Formel $x^2 - Ay^2$ dargestellt wird, auch durch $Ay^2 - x^2$ dargestellt werden kann. Denn da man $m^2 - An^2 = -1$ setzen kann, so hat man:

$$N = (x^2 - Ay^2)(An^2 - m^2) = A(my + nx)^2 - (mx + Any)^2.$$

44.

Ist zweitens A von der Form $8n + 3$, so kann die Gleichung (1), wie wir soeben gesehen haben, nicht stattfinden. Ebensowenig kann Gleichung (4) stattfinden. Denn wenn eine der Zahlen g und h gerade wäre, so würde die andere ebenfalls gerade sein, da die linke Seite gerade ist. Alsdann aber würde die rechte Seite durch 4 teilbar sein, während die linke nur durch 2 teilbar wäre. Wenn die Zahlen g und h alle beide ungerade wären, so würde die rechte Seite von der Form $8n + 1 - (8n + 3)(8n + 1)$ oder $8n - 2$ sein, was mit der linken nicht im Einklang stände. Mithin ist die Gleichung (2) die einzig mögliche; sie mufs demnach notwendigerweise stattfinden, und daraus ergiebt sich der folgende **Satz:**

Ist A eine Primzahl von der Form $8n + 3$, so ist die Gleichung

$$x^2 - Ay^2 = -2$$

immer möglich.

45.

Ist drittens A von der Form $8n + 7$, so findet man durch ähnliche Betrachtungen, dafs die Gleichung (4) die einzige ist, welche stattfinden kann, und daraus ergiebt sich der folgende Satz:

Ist A eine Primzahl von der Form $8n + 7$, so ist die Gleichung

$$x^2 - Ay^2 = +2$$

immer möglich.

Man beachte noch, dafs, wenn die beiden kleinsten, der Gleichung $m^2 - An^2 = \pm 2$ genügenden Zahlen m und n gegeben sind, es leicht ist, daraus die beiden Zahlen p und q, welche der Gleichung $p^2 - Aq^2 = 1$ genügen, herzuleiten. Dazu hat man zu setzen:

$$\frac{1}{2}(m + n\sqrt{A})^2 = p + q\sqrt{A}.$$

Dies giebt:

$$p = An^2 \pm 1, \qquad q = mn.$$



46.

Es sei jetzt $A = MN$, wo M und N zwei beliebige ungerade Primzahlen bezeichnen, und es seien ferner stets p und q die kleinsten Zahlen, welche der Gleichung

$$p^2 - Aq^2 = 1$$

genügen. Bringt man diese Gleichung auf die Form:

$$(p + 1)(p - 1) = MNq^2,$$

und setzt man $q = fgh$, so läſst sich dieselbe nur auf folgende vier Arten zerlegen:

$$p + 1 = fMg^2, \quad fNg^2, \quad fMNg^2, \quad fg^2$$
$$p - 1 = fNh^2, \quad fMh^2, \quad fh^2 \quad , \quad fMNh^2.$$

Hieraus folgen die vier Gleichungen:

$$\frac{2}{f} = Mg^2 - Nh^2 \quad ,$$
$$\frac{2}{f} = Ng^2 - Mh^2 \quad ,$$
$$\frac{2}{f} = MNg^2 - h^2 \quad ,$$
$$\frac{2}{f} = g^2 - MNh^2,$$

in denen man nach einander $f = 1$ und $f = 2$ zu setzen hat. Dies giebt die acht Kombinationen:

$$(1) \quad 1 = Mg^2 - Nh^2 \quad , \qquad (2) \quad 2 = Mg^2 - Nh^2$$
$$(3) \quad 1 = Ng^2 - Mh^2 \quad , \qquad (4) \quad 2 = Ng^2 - Mh^2$$
$$(5) \quad -1 = h^2 - MNg^2, \qquad (6) \quad -2 = h^2 - MNg^2$$
$$(7) \quad 1 = g^2 - MNh^2, \qquad (8) \quad 2 = g^2 - MNh^2.$$

Hiervon ist die siebente auszuschlieſsen, da nach Voraussetzung p und q die kleinsten der Gleichung $p^2 - Aq^2 = 1$ genügenden Zahlen sein sollen.

Wir geben jetzt zwei der hauptsächlichsten Folgerungen, welche man aus diesen Zerlegungen ziehen kann.

47.

Erstens: Wenn die Primzahlen M und N alle beide von der Form $4n + 3$ sind, so kann keine der Gleichungen (2), (4), (6), (8) stattfinden. Denn mag man die Zahlen g und h beliebig als gerade oder ungerade annehmen, stets wird die rechte Seite jener Gleichungen von einer der drei Formen $4n$, $4n + 1$, $4n + 3$ sein, während die linke Seite ± 2 ist. Bei derselben Voraussetzung kann

die Gleichung (5) ebensowenig stattfinden, denn wir werden später (No. 144) beweisen, dafs keine Zahl von der Form $4n + 3$ ein Teiler von $1 + h^2$ sein kann. Mithin mufs von den beiden übrigbleibenden Gleichungen (1) und (3) notwendigerweise die eine stattfinden, und daraus ergiebt sich folgender sehr bemerkenswerte **Satz:**

Wenn M und N zwei beliebige Primzahlen von der Form $4n + 3$ sind, so ist die Gleichung

$$Mx^2 - Ny^2 = \pm 1,$$

wenn man das Vorzeichen der rechten Seite passend bestimmt, stets möglich.

48.

Zweitens: Wenn die Primzahlen M und N alle beide von der Form $4n + 1$ sind, so erkennt man auf gleiche Weise, dafs die Gleichungen (2), (4), (6), (8) ebenfalls nicht stattfinden können. Dagegen ist die Gleichung (5) nicht mehr auszuschliefsen, und es kann somit der auf diesen Fall bezügliche Satz folgendermafsen ausgesprochen werden.

Sind M und N zwei Primzahlen von der Form $4n + 1$, so kann man immer entweder der Gleichung

$$x^2 - MNy^2 = -1$$

oder der Gleichung

$$Mx^2 - Ny^2 = \pm 1,$$

wenn man das Vorzeichen der letzteren passend annimmt, Genüge leisten.

Da man übrigens die Zerlegung der Zahlgröfse $p^2 - 1$ in zwei Faktoren $p + 1$ und $p - 1$, welche sich von einander nur um zwei Einheiten unterscheiden, nur auf eine einzige Weise vornehmen kann, so ist ersichtlich, dafs man niemals den beiden vorhergehenden Gleichungen gleichzeitig, sondern nur einer von ihnen genügen kann.

49.

Durch ganz ähnliche Betrachtungen gelangt man leicht zu einem noch weit allgemeineren **Satze**, nämlich zu dem folgenden:

Sind M und M' zwei Primzahlen von der Form $4n + 3$ und N eine Primzahl von der Form $4n + 1$, so ist es stets möglich, einer der sechs Gleichungen:

$$Nx^2 - MM'y^2 = \pm 1$$
$$Mx^2 - M'Ny^2 = \pm 1$$
$$M'x^2 - MNy^2 = \pm 1$$

zu genügen.

50.

Diese Sätze und andere ähnlicher Art lassen sich auch aus der Betrachtung des mittleren Quotienten, welchen die Entwicklung von $\sqrt{A}$ in einen Kettenbruch darbietet, ableiten.

Es bezeichne nämlich stets $\frac{p}{q}$ den einfachsten Bruch, welcher der Gleichung

$$p^2 - Aq^2 = 1$$

genügt; ferner sei a die gröſste in $\sqrt{A}$ enthaltene ganze Zahl, und es mögen aus der Entwicklung von $\sqrt{A}$ die Quotienten und die Näherungsbrüche bis zu $\frac{p}{q}$ folgendermaſsen entstehen:

Quotienten: $a, \ \alpha, \ \beta \cdots, \ \lambda, \ \vartheta, \ \lambda, \cdots \ \beta, \ \alpha, \ 2a, \cdots$

Näherungsbrüche: $\frac{1}{0}, \ \frac{a}{1}, \cdots, \frac{f^0}{g^0}, \ \frac{f}{g}, \ \frac{f'}{g'}, \cdots \ , \frac{p^0}{q^0}, \ \frac{p}{q}, \cdots$

Den mittelsten Quotienten haben wir mit ϑ bezeichnet. Ein solcher muſs notwendigerweise existieren, da sonst der Bruch $\frac{p}{q}$ von gerader Ordnung und somit gegen die Voraussetzung $p^2 - Aq^2 = -1$ sein würde. Da nun die Periode $\alpha, \ \beta, \ldots \vartheta, \ldots \beta, \ \alpha$ symmetrisch ist, so muſs der Bruch $\frac{g^0}{g}$ bei seiner Entwicklung die auf ϑ folgenden Quotienten $\lambda, \ldots \beta, \ \alpha$ ergeben (No. 11). Mithin kann man mit Hülfe des vollständigen Quotienten $\vartheta + \frac{g_0}{g}$ unmittelbar den Bruch $\frac{p}{q}$ aus den beiden aufeinanderfolgenden Brüchen $\frac{f^0}{g^0}, \ \frac{f}{g}$ ableiten, und zwar in folgender Weise:

$$\frac{p}{q} = \frac{f\left(\vartheta + \frac{g^0}{g}\right) + f^0}{g\left(\vartheta + \frac{g^0}{g}\right) + g^0}.$$

Hieraus folgt:

$$p = f(\vartheta g + 2g^0) + (f^0 g - f g^0)$$
$$q = g(\vartheta g + 2g^0).$$

Substituiert man diese Werte in die Gleichung:

$$p^2 - Aq^2 = 1 = (f^0 g - f g^0)^2,$$

so ergiebt sich:

$$(f^2 - Ag^2)(\vartheta g + 2g^0) = 2f(fg^0 - f^0 g).$$

Setzt man:

$$f^2 - Ag^2 = (fg^0 - f^0 g)D,$$



so wird:

$$\vartheta g + 2g^0 = \frac{2f}{D},$$

und hieraus erkennt man, daſs D ein Teiler sein muſs von $2f$.

51.

Ist erstens D gerade und gleich $2M$, so muſs $f = Mh$ sein und die Gleichung

$$f^2 - Ag^2 = (fg^0 - f^0g)D$$

geht über in:

$$M^2h^2 - Ag^2 = 2M(fg^0 - f^0g).$$

Nun kann aber g mit M keinen gemeinschaftlichen Teiler haben, da es sonst auch einen solchen mit $f = Mh$ haben würde; mithin ist M ein Teiler von A.

Ist also $A = MN$, so erhält man:

$$Mh^2 - Ng^2 = 2(fg^0 - f^0g) = \pm 2.$$

Demnach ist in diesem ersten Falle die Gleichung

$$Mx^2 - Ny^2 = \pm 2$$

möglich, wobei zu beachten ist, daſs, wenn die Zahlen M und N alle beide ungerade sind, die eine von der Form $4n + 1$, die andere von der Form $4n + 3$ sein muſs. Denn wären sie beide von der Form $4n + 1$ oder beide von der Form $4n + 3$, so würde die linke Seite durch 4 teilbar sein; sie könnte sich also nicht auf ± 2 reducieren.

Ist zweitens D ungerade und gleich M, so muſs man $f = Mh$ setzen. Dies giebt:

$$M^2h^2 - Ag^2 = \pm M.$$

Somit ist A ebenfalls teilbar durch M, und man erhält, wenn $A = MN$ gesetzt wird:

$$Mh^2 - Ng^2 = \pm 1.$$

Aus diesen beiden Fällen ergiebt sich der folgende **Satz:**

Ist eine beliebige, aber nicht quadratische Zahl A gegeben, so ist es immer möglich, diese Zahl in zwei Faktoren M und N von der Beschaffenheit zu zerlegen, daſs die eine der beiden Gleichungen

$$Mx^2 - Ny^2 = \pm 1$$
$$Mx^2 - Ny^2 = \pm 2$$

befriedigt wird, wenn man das Zeichen der rechten Seite passend wählt.

Ferner ist noch folgendes zu beachten:

1) Für eine und dieselbe Zahl $A = MN$ giebt es stets nur eine Art, einer dieser Gleichungen zu genügen; denn es ergiebt sich aus der Entwicklung von $\sqrt{A}$ in einen Kettenbruch nur ein mittelster Quotient.

2) Nimmt man $M = 1$, wodurch $N = A$ wird, so mufs man die Gleichung $x^2 - Ay^2 = 1$ ausscheiden, da man ihr durch kleinere Zahlen, wie $x = p$ und $y = q$ sind, nicht genügen kann. Es bleiben daher nur die drei Gleichungen:

$$x^2 - Ay^2 = -1, \quad x^2 - Ay^2 = 2, \quad x^2 - Ay^2 = -2,$$

und diese werden sehr häufig unmöglich sein, z. B. die erste, wenn einer der Primfaktoren von A von der Form $4n + 3$ ist, die zweite, wenn einer dieser Faktoren von der Form $8n + 5$ oder $8n + 3$ ist, und die dritte, wenn ein Faktor von der Form $8n + 5$ oder $8n + 7$ existiert.

Ist A eine Primzahl, so kann man keine andere Annahme machen, als $M = 1$ und $N = A$. Alsdann gelangt man durch Diskussion der Gleichungen $x^2 - Ay^2 = \pm 1$, $x^2 - Ay^2 = \pm 2$ zu denselben Sätzen wie oben hinsichtlich der Primzahlen von der Form $4n + 1$, $8n + 3$, $8n + 7$. Ebenso würde man diejenigen, welche auf die bereits behandelten Formen $A = MN$, $A = MM'N$ Bezug haben, erhalten.

52.

Ist die Gleichung

$$x^2 - Ay^2 = -1$$

auflösbar (dies findet statt nicht allein in dem Falle, wo A eine Primzahl von der Form $4n + 1$ ist, sondern noch in unendlich vielen andern Fällen), so hat man $D = 1$ und $\vartheta = 2a$. Daraus folgt, dafs die Quotienten $\alpha, \beta, \ldots$ bis λ eine symmetrische Reihe bilden (No. 33). Ferner mufs eben diese Reihe, da alsdann $f^2 - Ag^2 = -1$ ist, aus einer geraden Anzahl von Gliedern bestehen. Hiernach wird sich die Entwicklung von $\sqrt{A}$ in einen Kettenbruch bis zum Näherungsbruche $\frac{f}{g}$ hin folgendermafsen darstellen:

Quotienten: $\quad a\,, \quad \alpha\,, \beta, \ldots \quad \mu\,, \quad \mu\,, \ldots \beta, \quad \alpha\,, \quad 2a$

Näherungsbrüche: $\frac{1}{0}, \frac{a}{1}, \ldots\ldots \frac{m^0}{n^0}, \frac{m}{n}, \ldots\ldots, \frac{f^0}{g^0}, \frac{f}{g}.$

Nun kann man mit Hülfe der beiden aufeinanderfolgenden Brüche $\frac{m^0}{n^0}, \frac{m}{n}$, welche den mittleren Quotienten μ, μ entsprechen, unmittel-



bar den Wert von $\frac{f}{g}$ erhalten, nämlich:

$$\frac{f}{g} = \frac{m\left(\frac{n}{n^0}\right) + m^0}{n\left(\frac{n}{n^0}\right) + n^0} = \frac{mn + m^0 n^0}{n^2 + n^{0\,2}}.$$

Hieraus folgt:

$$f = mn + m^0 n^0$$

$$g = n^2 + n^{0\,2}.$$

Substituiert man diese Werte in die Gleichung:

$$f^2 - Ag^2 = -1 = -(mn^0 - m^0 n)^2,$$

und reduciert man diese, so erhält man:

$$A(n^2 + n^{0\,2}) = m^2 + m^{0\,2}$$

oder:

$$m^2 - An^2 = -(m^{0\,2} - An^{0\,2}).$$

Sind $\frac{\sqrt{A} + J^0}{D^0}$ und $\frac{\sqrt{A} + J}{D}$ die den Näherungsbrüchen $\frac{m^0}{n^0}$, $\frac{m}{n}$ entsprechenden vollständigen Quotienten, so hat man (No. 30):

$$m^2 - An^2 = (mn^0 - m^0 n)D,$$

und:

$$m^{0\,2} - An^{0\,2} = -(mn^0 - m^0 n)D^0.$$

Mithin:

$$D^0 = D.$$

Da aber allgemein

$$DD^0 + J^2 = A$$

ist, so folgt:

$$A = D^2 + J^2.$$

Allemal also, wenn die Gleichung $x^2 - Ay^2 = -1$ auflösbar ist (was unter andern stets dann stattfindet, wenn A eine Primzahl von der Form $4n + 1$ ist), läfst sich die Zahl A in zwei Quadrate zerlegen. Diese Zerlegung wird unmittelbar durch den vollständigen Quotienten $\frac{\sqrt{A} + J}{D}$ gegeben, welcher dem zweiten der mittleren in der ersten Periode der Entwicklung von $\sqrt{A}$ auftretenden Quotienten entspricht. Sind die Zahlen J und D auf diese Weise bekannt, so erhält man $A = D^2 + J^2$.

Dieser Schlufs enthält einen der **schönsten Sätze** der Zahlentheorie, nämlich:

„Jede Primzahl von der Form $4n + 1$ ist die Summe zweier Quadrate.“

Derselbe giebt zugleich das Mittel an die Hand, um diese Zerlegung auf direktem Wege und ohne jedes Probieren auszuführen.

§ 8.

Zurückführung der Formel $Ly^2 + Myz + Nz^2$ auf den einfachsten Ausdruck.

53.

Die Koefficienten L, M, N in dieser Formel werden als gegebene Zahlen (jedoch von der Art, dafs sie nicht alle drei durch eine und dieselbe Zahl teilbar sind) angenommen; die Gröfsen y und z dagegen sind unbestimmte Zahlen, denen man alle möglichen positiven oder negativen ganzzahligen Werte unter der einzigen Einschränkung, dafs y und z prim zu einander sein sollen, beilegen kann. Es wird daher stets unendlich viele Zahlen geben, welche durch dieselbe Formel $Ly^2 + Myz + Nz^2$ dargestellt werden. Im Allgemeinen aber kann diese Formel verschiedene Formen, welche alle dieselben Zahlen unter sich begreifen, annehmen, und es handelt sich nunmehr darum, den **einfachsten Ausdruck** aller dieser Formen zu bestimmen.

Wir werden zunächst den Fall betrachten, wo M eine **gerade** Zahl ist, weil dieser die meiste Anwendung findet; sodann werden wir die analogen Resultate, welche gelten, wenn M ungerade ist, angeben.

Ist also die Formel

$$py^2 + 2qyz + rz^2$$

gegeben, in welcher p, q, r gegebene Zahlen sind, und will man diese Formel in eine andere umwandeln, die sich von ihr nur durch die Koefficienten unterscheidet, so mufs man setzen:

$$y = fy' + mz'$$
$$z = gy' + nz',$$

wobei y' und z' neue unbestimmte Zahlen sind. Hiernach giebt die Einsetzung dieser Werte die transformierte Formel:

$$p'y'^2 + 2q'y'z' + r'z'^2,$$

deren Koefficienten sind:

$$p' = pf^2 + 2qfg + rg^2$$
$$q' = pfm + q(fn + gm) + rgn$$
$$r' = pm^2 + 2qmn + rn^2.$$



Damit nun die Koefficienten f, g, m, n den Bereich der Unbestimmten y und z in der gegebenen Formel nicht beschränken, ist erforderlich, dafs die Werte von y' und z', ausgedrückt durch y und z, nämlich

$$y' = \frac{ny - mz}{fn - mg}$$

$$z' = \frac{fz - gy}{fn - mg},$$

ganze Zahlen seien, und zwar unabhängig von jedem besonderen Werte von y und z. Dazu mufs also sein:

$$fn - mg = \pm 1.$$

Daraus erkennt man, dafs man zwei Koefficienten, etwa f und g, willkürlich annehmen kann, vorausgesetzt, dafs sie prim zu einander sind. Nimmt man sodann für $\frac{m}{n}$ den Näherungsbruch, welcher $\frac{f}{g}$ in der Entwicklung des letzteren Bruches in einen Kettenbruch vorhergeht, so ist hierdurch die Bedingung $fn - mg = \pm 1$ erfüllt, und man kann sicher sein, dafs jede Zahl, welche in der Formel

$$py^2 + 2qyz + rz^2$$

enthalten ist, auch in ihrer Transformation

$$p'y'^2 + 2q'y'z' + r'z'^2$$

enthalten ist und umgekehrt. Da ferner y und z nach Voraussetzung prim zu einander sind, so müssen es y' und z' ebenfalls sein; denn hätten y' und z' einen gemeinschaftlichen Teiler ϑ, so würden die Zahlen y und z ebenfalls (den Werten $y = fy' + mz'$, $z = gy' + nz'$ zufolge) durch ϑ teilbar sein, was im Widerspruch steht mit der Voraussetzung.

Wir bemerken ferner, dafs die für p', q', r' gefundenen Werte die Gleichung ergeben:

$$p'r' - q'^2 = (pr - q^2)(fn - mg)^2 = pr - q^2,$$

woraus folgt, dafs „die Gröfse $pr - q^2$ und die ihr entsprechende $p'r' - q'^2$ in der transformierten Formel gleich und von gleichem Zeichen sind“.

Diese Gröfse $pr - q^2$ bestimmt die **besondere Beschaffenheit** der Formel $py^2 + 2qyz + rz^2$ rücksichtlich der beiden Faktoren $\alpha y + \beta z$, $\gamma y + \delta z$, aus denen man sich dieselbe zusammengesetzt denken kann. Wenn diese Faktoren imaginär sind, so ist die Gröfse $pr - q^2$ positiv; sind dieselben entweder gleich oder rational, so ist die Gröfse $pr - q^2$ gleich 0 bezw. gleich einer negativen Quadratzahl. Sind sie endlich reell, aber irrational, so ist die Gröfse $pr - q^2$

gleich einer negativen, nichtquadratischen Zahl. Man erkennt dies, wenn man die Formel $py^2 + 2qyz + rz^2$ auf die Form bringt:

$$\frac{1}{p}[py + qz + z\sqrt{q^2 - rp}]\ [py + qz - z\sqrt{q^2 - pr}].$$

Wir werden diese verschiedenen Fälle getrennt von einander untersuchen. Vor allem andern aber müssen wir folgende **allgemeine Aufgabe***) lösen.

54.

Ist die unbestimmte Formel $py^2 + 2qyz + rz^2$ gegeben, in welcher der mittlere Koefficient $2q$ **gröſser** ist als einer der beiden äuſseren Koefficienten p und r oder auch gröſser als alle beide, so soll man diese Formel in eine andere ähnliche transformieren, in welcher der mittlere Koefficient **kleiner** als jeder der äuſseren oder wenigstens nicht gröſser als der kleinste der beiden letzteren ist.

Wir setzen $2q > p$ voraus, und in dem Falle, wo zugleich $2q > p$ und $2q > r$ ist, sei p die kleinere der beiden Zahlen p und r, abgesehen von ihren Vorzeichen. Setzen wir:

$$y = y' - mz,$$

wo m ein noch unbestimmter Koefficient ist, so ergiebt die Substitution dieses Wertes die transformierte Formel:

$$py'^2 - (2pm - 2q)y'z + (pm^2 - 2qm + r)z^2.$$

Die unbestimmte Zahl m kann man derart annehmen, daſs $2pm - 2q$ kleiner als p oder gleich p ist. Dazu muſs m die ganze Zahl sein, welche dem gegebenen Bruche $\frac{q}{p}$, sei es nach oben oder unten hin, am nächsten liegt. Setzt man sodann:

$$pm - q = q', \quad pm^2 - 2qm + r = r',$$

so wird die transformierte Formel:

$$py'^2 - 2q'y'z + r'z^2,$$

und es ist:

$$pr' - q'^2 = pr - q^2, \text{ und } 2q' < p,$$

wobei das Zeichen $<$ die Gleichheit nicht ausschlieſst.

Da nun gleichzeitig

$$2q > p \text{ und } 2q' < p$$

ist, so folgt daraus:

$$q' < q.$$

*) Die Lösung dieser Aufgabe, einer der wichtigsten in der unbestimmten Analysis, verdankt man Lagrange. Siehe Abhandlungen der Berliner Akademie vom Jahre 1773. Anm. d. Verf.



Dies ist das Hauptziel dieser ersten Rechnung. Wenn jetzt in dieser transformierten Formel der Koefficient $2q'$ obwohl kleiner als p, noch gröfser als r' ist, so kann man ebenso verfahren, und wird dadurch eine neue transformierte Formel erhalten, in welcher der mittlere Koefficient, welcher $2q''$ heifsen möge, kleiner als $2q'$ ist. Nun kann eine Reihe abnehmender ganzer Zahlen $q, q', q'', q''', \ldots$ nicht ins Unendliche fortgehen; setzt man demnach dieselben Rechnungen weiter fort, so gelangt man notwendig zu einer transformierten Formel, bei welcher es eine weitere Reduktion nicht mehr giebt, und die demnach so beschaffen sein wird, dafs der mittlere Koefficient keinen der beiden äufseren übersteigt. Diese transformierte Formel leistet der gestellten Aufgabe Genüge; die in ihr vorkommenden unbestimmten Zahlen werden ebenfalls prim zu einander sein und die $pr - q^2$ entsprechende Gröfse wird denselben Wert und dasselbe Vorzeichen besitzen, wie in der gegebenen Formel. Denn diese beiden Bedingungen sind, wie wir gezeigt haben, beim Übergange von einer transformierten Formel zur andern immer erfüllt.

Wir wollen als Beispiel die Formel

$$35y^2 + 172yz + 210z^2$$

betrachten. Da die dem Bruche $\frac{q}{p} = \frac{86}{35}$ am nächsten liegende ganze Zahl 2 ist, so setze man:

$$y = y' - 2z.$$

Dies giebt die transformierte Formel:

$$35y'^2 \left.\begin{matrix} -140 \\ +172 \end{matrix}\right\} y'z \left.\begin{matrix} +140 \\ -344 \\ +210 \end{matrix}\right\} z^2 = 35y'^2 + 32y'z + 6z^2.$$

Da in dieser der mittlere Koefficient 32 gröfser ist als der äufsere Koefficient 6, so mufs man in derselben Weise zu einer neuen transformierten Formel übergehen. Nimmt man also die dem Bruche $\frac{16}{6}$ am nächsten liegende ganze Zahl, welche 3 ist, und setzt man:

$$z = z' - 3y',$$

so wird die neue transformierte Formel:

$$6z'^2 \left.\begin{matrix} -36 \\ +32 \end{matrix}\right\} z'y' \left.\begin{matrix} +54 \\ -96 \\ +35 \end{matrix}\right\} y'^2 = 6z'^2 - 4z'y' - 7y'^2.$$

Diese letztere erfüllt die verlangten Bedingungen, da der mittlere Koefficient 4 kleiner ist als jeder der äufseren 6 und 7. Zugleich sieht man, dafs die Gröfse $pr - q^2$ in der gegebenen Formel ebenso wie in der transformierten gleich -46 ist. Was die Beziehung zwischen den ersten Veränderlichen y und z und den neuen y' und z' anlangt, so findet man, dafs dieselbe durch die Gleichungen

$$y = 7y' - 2z'$$
$$z = z' - 3y'$$

gegeben ist.

Wir untersuchen jetzt die drei allgemeinen Fälle, deren wir oben (No. 53) Erwähnung gethan.

55.

Ist erstens $pr - q^2$ gleich einer **negativen** Zahl $-A$, so können wir annehmen, dafs die Formel $py^2 + 2qyz + rz^2$ auf die einfachste Form gebracht sei, so dafs $2q$ weder p noch r übersteigt. Alsdann aber behaupte ich, dafs die Zahlen p und r von verschiedenen Vorzeichen sind. Denn hätten sie dasselbe Zeichen, so würde pr positiv und $> 4q^2$, demnach $pr - q^2$ positiv und $> 3q^2$ sein, und diese Gröfse könnte somit nicht gleich $-A$ sein. Wir können daher voraussetzen, dafs die in Rede stehende Formel die folgende sei:

$$ay^2 + 2byz - cz^2,$$

wo a und c positiv und $ac + b^2 = A$ ist. Ferner aber hat man stets $2b < a$ und $2b < c$, folglich $ac + b^2 > 5b^2$, und daher $5b^2 < A$, oder

$$b < \sqrt{\frac{A}{5}}\,.$$

Zu gleicher Zeit sind die Grenzen von ac:

$$ac < A, \quad ac > \frac{4}{5}A.$$

Bemerkung. Es kann vorkommen, dafs verschiedene derartige Formeln wie $ay^2 + 2byz - cz^2$ einem und demselben Werte von A zugehören und zugleich der Bedingung $2b < a$ und $2b < c$ genügen, ohne dafs sie jedoch wesentlich von einander verschieden wären. So geben z. B. die beiden Formeln:

$$y^2 - 7z^2$$

und:

$$2y^2 + 2yz - 3z^2$$

in gleicher Weise $ac + b^2 = 7$ und $2b < a$ und $< c$. Setzt man indessen:

$$y = 2t - 5u, \quad z = 3u - t,$$

so geht die Formel $2y^2 + 2yz - 3z^2$ in $t^2 - 7u^2$ über, und setzt man umgekehrt in dieser letzteren:

$$t = 3y + 5z, \quad u = y + 2z,$$

so verwandelt sie sich in die erstere $2y^2 + 2yz - 3z^2$. Daraus erkennt man, dafs diese beiden Formeln in Wirklichkeit nur zwei verschiedene Ausdrücke einer und derselben Formel sind, und dafs es keine in der einen von ihnen enthaltene Zahl giebt, die nicht auch mit demselben Werte und demselben Zeichen in der andern enthalten wäre.

Ist die Zahl A gegeben, so kann man leicht alle Formeln $ay^2 + 2byz - cz^2$ finden, welche den Bedingungen $b^2 + ac = A$, $2b < a$ und $< c$ genügen, und es ist klar, dafs die **Anzahl** dieser Formeln notwendig **beschränkt** ist, da a und c positiv und $b < \sqrt{\frac{A}{5}}$ sein mufs. Nachdem man aber diese verschiedenen Formeln gefunden hat, hat man noch diejenigen abzuscheiden, welche nicht wesentlich von einander verschieden sind, um die Gesamtheit auf die kleinstmögliche Anzahl reducieren zu können. Diese Untersuchung wird uns im § 13 beschäftigen.

Ist zweitens unter der beständigen Voraussetzung, dafs

$$pr - q^2 = -A$$

sei, A ein **vollständiges Quadrat**, so ist die gegebene Formel

$$py^2 + 2qyz + rz^2$$

in zwei rationale Faktoren $(\alpha y + \beta z)(\gamma y + \delta z)$ zerlegbar. Hat man ferner $pr - q^2 = 0$, so sind diese beiden Faktoren einander gleich. Diese Fälle bedürfen keiner weiteren Auseinandersetzung, und man erkennt leicht, welches alsdann der einfachste Ausdruck der gegebenen Formel ist.

Ist daher drittens $pr - q^2$ gleich einer **positiven** Zahl A, und setzen wir wiederum voraus, dafs die Formel $py^2 + 2qyz + rz^2$ auf ihren einfachsten Ausdruck gebracht sei, so dafs $2q$ weder p noch r übersteigt, so hat man $pr > 4q^2$ und $3q^2 < A$ oder:

$$q < \sqrt{\frac{A}{3}}.$$

Zugleich sieht man, dafs pr stets zwischen den Grenzen A und $\frac{4}{3}A$ enthalten ist.

Ist die Zahl A gegeben, so kann man leicht alle Formeln

$py^2+2qyz+rz^2$ finden, welche den Bedingungen $pr-q^2=A$ und $2q<p$ und $<r$ genügen. Man kann ferner beweisen, dafs alle diese Formeln wesentlich von einander verschieden sind und sich nicht auf eine geringere Anzahl reducieren lassen. Dies wird durch die beiden folgenden Sätze geschehen.

56.

Satz. Wenn die unbestimmte Formel $py^2+2qyz+rz^2$ so beschaffen ist, dafs $2q$ weder p noch r übersteigt, und wenn zugleich $pr-q^2$ gleich einer positiven Zahl A ist, so behaupte ich, dafs die beiden **kleinsten** in dieser Formel enthaltenen Zahlen p und r sind.

Man beachte zuerst, dafs die Formel $py^2+2qyz+rz^2$, analytisch betrachtet, dieselbe ist wie $py^2-2qyz+rz^2$, da man nach Belieben die Unbestimmten y und z positiv oder negativ nehmen kann. Nun ist, unter übrigens gleichen Umständen,

$$py^2+2qyz+rz^2,$$

worin wir die drei Glieder positiv annehmen, gröfser als

$$py^2-2qyz+rz^2;$$

mithin kann nur in Bezug auf diese letztere das Minimum stattfinden.

Es sei also $P=py^2-2qyz+rz^2$ und $y>z$. Setzen wir $y-1$ an die Stelle von y und nehmen wir an, dafs P in P' übergehe, so erhalten wir:

$$P'=P-2py+p+2qz$$

oder:

$$P'=P-2q(y-z)-y(p-2q)-p(y-1).$$

Wegen $p>2q$ und $y>z$ ist aber offenbar P' kleiner als P, selbst wenn, wie wir immer voraussetzen, das Zeichen $>$ auch die Gleichheit mit einschliefst.

Man könnte einwerfen, dafs, wenn auch $P'=P-Q$, wo Q eine positive Gröfse ist, doch, im Falle Q selbst gröfser als P wäre, P' einen negativen Wert haben könnte, der gröfser als P wäre. Dieser Einwurf fällt von selbst, wenn man beachtet, dafs es keinen Wert von y und z giebt, für welchen die Formel $py^2-2qyz+rz^2$ negativ würde, da seine Faktoren imaginär sind.

Es folgt hieraus, dafs man, welches auch die Werte von y und z, die das Resultat P geben, sein mögen, ein kleineres Resultat findet, wenn man die gröfste der beiden Zahlgröfsen y und z oder, im Falle sie gleich, die eine von ihnen um eine Einheit vermindert. Der von uns gemachte Schlufs würde nämlich ebenfalls gelten, wenn $y=z$

wäre. Verkleinert man aber die Unbestimmten y und z in derselben Weise weiter, so gelangt man notwendig zu den Werten $y = 1$ und $z = 1$. Mithin ist die Gröfse $P = p - 2q + r$, welche den Werten $y = 1$, $z = 1$ entspricht, kleiner als alle diejenigen, welche zu gröfseren Werten dieser Veränderlichen gehören.

Andrerseits aber ist die Zahlgröfse $p - 2q + r$, da $2q < p$ und $< r$ ist, gröfser oder mindestens gleich der gröfsten der beiden Zahlen p und r. Folglich sind die beiden Zahlen p und r die kleinsten in der gegebenen Formel enthaltenen Zahlen, und nächst diesen ist die kleinste: $p - 2q + r$.

57.

Satz. Wenn zwei unbestimmte Formeln $py^2 + 2qyz + rz^2$ und $p'y^2 + 2q'yz + r'z^2$ beide so beschaffen sind, dafs der Koefficient des mittleren Gliedes keinen der äufseren Koefficienten übersteigt, und wenn zugleich die Gröfsen $pr - q^2$ und $p'r' - q'^2$ einer und derselben positiven Zahl A gleich sind, so behaupte ich, dafs diese **beiden** Formeln wesentlich von einander **verschieden** sind und sich nicht auf eine und dieselbe Formel reducieren lassen.

Denn wenn es möglich wäre, die eine von diesen Formeln in die andere zu transformieren, so müfste die eine von beiden mindestens eine Zahl in sich enthalten, welche kleiner als einer ihrer äufseren Koefficienten wäre. Dies verstöfst aber gegen den vorhergehenden Satz.

58.

Bisher haben wir die Formel $Ly^2 + Myz + Nz^2$ nur für den Fall betrachtet, wo der mittlere Koefficient M eine gerade Zahl ist. Setzen wir jetzt voraus, dafs dieser Koefficient eine **ungerade** Zahl sei, so findet man durch ähnliche Betrachtungen die folgenden Resultate, die wir uns begnügen anzuführen:

1) Jede unbestimmte Formel $Ly^2 + Myz + Nz^2$, in welcher $M > 2L$ ist, läfst sich auf eine ähnliche Formel zurückführen, in welcher der mittlere Koefficient kleiner als $2L$ ist, und in welcher die zu $4LN - M^2$ analoge Gröfse denselben Wert und dasselbe Zeichen besitzt wie diese. Dazu mufs man $y = y' - mz$ setzen und für m die ganze Zahl nehmen, welche $\frac{M}{2L}$ am nächsten liegt.

2) Mithin kann man mittelst einer oder mehrerer derartiger Transformationen die gegebene Formel in eine ähnliche umwandeln, in welcher der Koefficient des mittleren

Gliedes keinen der äufseren übersteigt, und in welcher die Gröfse $4LN - M^2$ denselben Wert und dasselbe Zeichen, wie in der gegebenen, besitzt.

3) Wenn $4LN - M^2$ gleich einer negativen Zahl $-B$ ist, so ist die transformierte Formel, welche den vorhergehenden Bedingungen genügt, von der Form $ay^2 + byz - cz^2$, wobei $B = b^2 + 4ac$, $b < a$ und $< c$ und folglich $b < \sqrt{\frac{B}{5}}$ ist.

Ist die Zahl B gegeben, so kann man leicht alle Formeln $ay^2 + byz - cz^2$ finden, welche den Bedingungen $b^2 + 4ac = B$, $b < a$ und $< c$ Genüge leisten. Jedoch können mehrere von diesen Formeln identisch oder in einander transformierbar sein. Dies soll im § 13 näher untersucht werden.

4) Wenn $4LN - M^2$ gleich einer positiven Zahl B ist, so ist die transformierte Formel $ay^2 + byz + cz^2$, welche den vorerwähnten Bedingungen $4ac - b^2 = B$, $b < a$ und $< c$ und somit $b < \sqrt{\frac{B}{3}}$ genügt, von der Beschaffenheit, dafs a und c die beiden kleinsten darin enthaltenen Zahlen sind.

Mithin sind alle Formeln dieser Art, welche einer und derselben gegebenen Zahl B zugehören, wesentlich von einander verschieden, und sie lassen sich nicht auf eine geringere Anzahl reducieren.

§ 9.

Entwicklung der Wurzel einer Gleichung zweiten Grades in einen Kettenbruch.

59.

Ist die Gleichung

$$fx^2 + gx + h = 0$$

gegeben, in welcher die Koefficienten **ganze** Zahlen und die Wurzeln **reell** sind, so soll die eine dieser Wurzeln, die wir der Einfachheit halber als positiv betrachten (wäre sie negativ, so könnte man $-x$ an Stelle von x setzen und dem Resultat das Zeichen $-$ vorsetzen), in einen Kettenbruch entwickelt werden.

Nachdem man anfangs nach der allgemeinen Methode gerechnet hat, nehme man an, dafs man bis zu den aufeinanderfolgenden Näherungsbrüchen $\frac{p^0}{q^0}$, $\frac{p}{q}$ gelangt sei. Ist z der diesem letzteren entsprechende vollständige Quotient, so erhält man:



$$x = \frac{pz + p^0}{qz + q^0},$$

und folglich:

$$z = \frac{q^0 x - p^0}{p - qx}.$$

Setzt man für x seinen Wert

$$x = \frac{-g + \sqrt{g^2 - 4fh}}{2f}$$

ein, so ergiebt sich:

$$z = \frac{-gq^0 - 2fp^0 + q^0\sqrt{g^2 - 4fh}}{gq + 2fp - q\sqrt{g^2 - 4fh}},$$

und dieser Ausdruck geht dadurch, dafs man den Nenner rational macht, über in:

$$z = \frac{\frac{1}{2}(pq^0 - p^0q)\sqrt{g^2 - 4fh} - fpp^0 - \frac{1}{2}g(pq^0 + p^0q) - hqq^0}{fp^2 + gpq + hq^2}.$$

Stellt man diesen Wert zur Abkürzung durch die Formel

$$z = \frac{\sqrt{A} + J}{D}$$

dar, so werden die Gröfsen A, J, D folgendermafsen sich ausdrücken:

$$A = \frac{1}{4}(g^2 - 4fh)$$
$$(pq^0 - p^0q)J = -fpp^0 - \frac{1}{2}g(pq^0 + p^0q) - hqq^0$$
$$(pq^0 - p^0q)D = fp^2 + gpq + hq^2,$$

woraus man erkennt, dafs wegen $pq^0 - p^0q = \pm 1$ die Zahl D stets eine ganze Zahl ist. Was die Zahl J betrifft, so wird sie eine ganze Zahl sein, wenn g gerade ist; sie wird dagegen stets den Bruch $\frac{1}{2}$ enthalten, wenn g ungerade ist.

60.

Wie weit man auch die Entwicklung von x in einen Kettenbruch fortgesetzt haben möge, der vollständige Quotient z drückt sich, wie man sieht, leicht mittelst der beiden letzten Näherungsbrüche $\frac{p^0}{q^0}$, $\frac{p}{q}$ aus. Dies könnte dazu dienen, die Entwicklung noch weiter fortzusetzen. Indessen kann man unabhängig von den Näherungsbrüchen das Fortschreitungsgesetz der vollständigen Quotienten erhalten. Es seien nämlich

$$\frac{\sqrt{A} + J^0}{D^0}, \quad \frac{\sqrt{A} + J}{D}, \quad \frac{\sqrt{A} + J'}{D'}$$

drei von diesen aufeinanderfolgenden Quotienten und

$$\frac{p^0}{q^0},\quad \frac{p}{q},\quad \frac{p'}{q'}$$

die ihnen entsprechenden Näherungsbrüche. Setzt man zur Abkürzung:

$$pq^0 - p^0q = i,$$

so erhält man, wie eben gefunden wurde:

$$iJ = -fpp^0 - \frac{1}{2}g(pq^0 + p^0q) - hqq^0$$

$$iD = \quad fp^2 \ + gpq + hq^2.$$

Geht man von hier aus zu den folgenden Werten über, und beachtet man dabei, dafs aldann i sein Zeichen ändert, da

$$p'q - pq' = -(pq^0 - p^0q)$$

ist, so werden diese Formeln:

$$-iJ' = -fp'p - \frac{1}{2}g(p'q + pq') - hq'q$$

$$-iD' = \quad fp'^2 \ + gp'q' + hq'^2.$$

Nennt man nun wie gewöhnlich μ den Quotienten, welcher dem Bruche $\frac{p}{q}$ entspricht, so hat man:

$$p' = \mu p + p^0, \quad q' = \mu q + q^0,$$

und diese Werte geben in die erste Gleichung eingesetzt:

$$iJ' = \mu(fp^2 + gpq + hq^2) + fpp^0 + \frac{1}{2}g(pq^0 + p^0q) + hqq^0$$

oder:

$$iJ' = \mu iD - iJ,$$

so dafs man ohne jede Mehrdeutigkeit erhält:

$$J' = \mu D - J.$$

Führt man dieselben Substitutionen in der Gleichung für D' aus, so erhält man in gleicher Weise:

$$-iD' = \mu^2(fp^2 + gpq + hq^2) + \mu(2fpp^0 + gp^0q + gpq^0 + 2hqq^0)$$
$$+ fp^{0\,2} + gp^0q^0 + hq^{0\,2},$$

und da die rechte Seite sich auf $\mu^2 iD - 2\mu iJ - iD^0$ reduciert, so ergiebt sich ebenfalls ohne Mehrdeutigkeit:

$$D' = D^0 + 2\mu J - \mu^2 D,$$

oder:

$$D' = D^0 + \mu(J - J').$$

Hieraus folgt, dafs, wenn zwei aufeinanderfolgende vollständige Quotienten

$$\frac{\sqrt{A}+J^0}{D^0} = \mu^0 +$$

$$\frac{\sqrt{A}+J}{D} = \mu +$$

gegeben sind, der nächstfolgende $\frac{\sqrt{A}+J'}{D'}$ sich sehr einfach durch die Werte

$$J' = \mu D - J$$
$$D' = D^0 + \mu(J - J')$$

bestimmt. Es ist dies dasselbe Gesetz, welches wir bei der Entwicklung der Quadratwurzeln (No. 29) gefunden hatten.

61.

Eliminiert man μ aus den beiden vorhergehenden Formeln, so erhält man:

$$D'D + J'^2 = DD^0 + J^2.$$

Nun enthält aber die linke Seite dieser Gleichung dieselben Gröfsen wie die rechte, mit dem einzigen Unterschiede, dafs erstere von einer um eine Einheit höheren Ordnung sind. Mithin mufs jede Seite eine konstante Gröfse sein. Um diese Gröfse als Funktion der Koefficienten der gegebenen Gleichung zu bestimmen, sei mit k die gröfste in x enthaltene ganze Zahl bezeichnet. Dann beginnt die Entwicklung des Wertes von x in folgender Weise:

$$x = \frac{\sqrt{A} - \frac{1}{2}g}{f} = k + \frac{\sqrt{A} - \frac{1}{2}g - fk}{f}$$

$$\frac{f}{\sqrt{A} - \frac{1}{2}g - fk} = \frac{\sqrt{A} + \frac{1}{2}g + fk}{-fk^2 - gk - h} = \text{u. s. w.}$$

Demnach kann man mit Rücksicht auf die beiden ersten vollständigen Quotienten

$$D^0 = f, \quad D = -fk^2 - gk - h$$
$$J = \frac{1}{2}g + fk$$

setzen. Dies giebt:

$$D^0 D + J^2 = \frac{1}{4}g^2 - fh = A.$$

Welches also auch die Ordnung des vollständigen Quotienten $\frac{\sqrt{A}+J}{D}$ sein möge, es ist allgemein:

$$D^0 D + J^2 = A.$$

Es kann vorkommen, dafs die ersten Werte von D abwechselnd positiv und negativ sind. Denn obwohl x immer zwischen zwei aufeinanderfolgenden Näherungsbrüchen $\frac{p^0}{q^0}$, $\frac{p}{q}$ liegt, so ist doch leicht zu sehen, dafs, wenn die beiden Wurzeln der Gleichung

$$fx^2 + gx + h = 0$$

weniger von einander verschieden sind, als diese beiden Näherungsbrüche von einander, die beiden Resultate

$$fp^{0\,2} + gp^0q^0 + hq^{0\,2}$$
$$fp^2 + gpq + hq^2,$$

welche man erhält, indem man in der linken Seite der Gleichung $\frac{p^0}{q^0}$ und $\frac{p}{q}$ an die Stelle von x setzt, notwendigerweise von demselben Zeichen und somit D^0 und D von verschiedenen Zeichen sind. Da jedoch die Annäherung mit Hülfe der Kettenbrüche sehr schnell zunimmt, so kann diese Abwechslung der Zeichen nur bei einer kleinen Anzahl der ersten Glieder stattfinden, und es werden bald die Gröfsen D beständig dasselbe Vorzeichen besitzen.

Rechnet man von diesem Punkte aus, wo die Reihe der vollständigen Quotienten eine regelmäfsigere Form annimmt, so erhält man, da die Gröfse DD^0 immer positiv ist, zu gleicher Zeit:

$$J < \sqrt{A} \text{ und } D < 2\sqrt{A}.$$

Da somit die Werte von J und D in dieser Weise beschränkt und da ferner $2J$ und D stets ganze Zahlen sind, so kann der vollständige Quotient $\frac{\sqrt{A}+J}{D}$ nur eine bestimmte Anzahl von verschiedenen Werten haben. Mithin mufs man nach einer mehr oder minder grofsen Anzahl von Gliedern, die jedoch $\sqrt{A} \times 2\sqrt{A}$ nicht übersteigen kann, notwendig auf einen bereits gefundenen vollständigen Quotienten stofsen, so dafs hiernach der Rest des Kettenbruches nur noch aus derselben Reihe oder Periode von bereits gefundenen Quotienten, die sich bis ins Unendliche wiederholt, besteht.

62.

Es giebt somit **unendlich viele** Näherungsbrüche $\frac{p}{q}$, $\frac{p_1}{q_1}$, $\frac{p_2}{q_2}$, $\cdots$, welche in den aufeinanderfolgenden Perioden einem und demselben vollständigen Quotienten $\frac{\sqrt{A}+J}{D}$ entsprechen,

und es ist von um so gröfserer Wichtigkeit, den **allgemeinen Ausdruck** dieser Brüche zu suchen, da sie dazu dienen, unendlich viele Auflösungen der Gleichungen von der Form

$$fy^2 + gyz + hz^2 = \pm D$$

zu liefern.

Es sei also $\mu, \mu', \mu'', \ldots \omega$ die Periode der Quotienten, welche unendlich oftmal wiederholt die Entwicklung von $\frac{\sqrt{A}+J}{D}$ bildet. Mittelst dieser Quotienten setze man die Berechnung der Näherungsbrüche von x in folgender Weise fort:

$$\begin{array}{llllllllllll} \text{Quotienten:} & & \mu, & \mu', & \cdots & \omega, & \mu, & \mu', \cdots & \omega, & \mu, & \mu' \cdots \\ \text{Näherungsbrüche:} & \frac{p^0}{q^0}, & \frac{p}{q}, & \frac{p'}{q'}, & \cdots & \frac{p_1{}^0}{q_1{}^0}, & \frac{p_1}{q_1}, & \cdots\cdot & \frac{p_2{}^0}{q_2{}^0}, & \frac{p_2}{q_2}, & \cdots\cdot \end{array}$$

Ferner bezeichne man mit $\frac{\alpha}{\beta}$ den Wert des Kettenbruches:

$$\mu + \frac{1}{\mu' + \frac{1}{\mu'' + \cdots}},$$

und zwar berechnet bis zum Gliede ω einschliefslich. Da man nun, welches auch der Wert von μ sei,

$$\frac{p'}{q'} = \frac{p\mu + p^0}{q\mu + q^0}$$

hat, so ist ebenso, wenn man $\frac{\alpha}{\beta}$ an Stelle von μ setzt:

$$\frac{p_1}{q_1} = \frac{p\frac{\alpha}{\beta} + p^0}{q\frac{\alpha}{\beta} + q^0} = \frac{p\alpha + p^0\beta}{q\alpha + q^0\beta}.$$

Dies giebt:

$$p_1 = p\alpha + p^0\beta$$
$$q_1 = q\alpha + q^0\beta.$$

Setzte man $\frac{\sqrt{A}+J}{D}$ an die Stelle μ, so würde man ebenso erhalten:

$$x = \frac{p\left(\frac{\sqrt{A}+J}{D}\right) + p^0}{q\left(\frac{\sqrt{A}+J}{D}\right) + q^0} = \frac{p\sqrt{A} + pJ + p^0D}{q\sqrt{A} + qJ + q^0D} = \frac{\sqrt{A} - \frac{1}{2}g}{f}.$$

Diese Gleichung würde dieselben Werte von J und D geben, die wir oben gefunden haben. Man erhält ferner daraus unmittelbar:

$$p^0 = -\frac{p}{D}\left(\frac{1}{2}g + J\right) - \frac{hq}{D}$$
$$q^0 = \quad \frac{q}{D}\left(\frac{1}{2}g - J\right) + \frac{fp}{D}.$$

Setzt man diese Werte in die Werte von p_1 und q_1 ein, so folgt:

$$p_1 = p\left(\alpha - \frac{\beta}{D}J - \frac{\beta}{D}\cdot\frac{1}{2}g\right) - \frac{\beta}{D}hq$$

$$q_1 = q\left(\alpha - \frac{\beta}{D}J + \frac{\beta}{D}\cdot\frac{1}{2}g\right) + \frac{\beta}{D}fp.$$

In analoger Weise erhält man demnach, wegen der Gleichheit der Perioden:

$$p_2 = p_1\left(\alpha - \frac{\beta}{D}J - \frac{\beta}{D}\cdot\frac{1}{2}g\right) - \frac{\beta}{D}hq_1$$

$$q_2 = q_1\left(\alpha - \frac{\beta}{D}J + \frac{\beta}{D}\cdot\frac{1}{2}g\right) + \frac{\beta}{D}fp_1.$$

Setzt man zur Abkürzung:

$$\alpha - \frac{\beta}{D}J = \varphi, \quad \frac{\beta}{D} = \psi, \quad \varphi^2 - A\psi^2 = \varepsilon,$$

so ergiebt sich aus diesen Gleichungen:

$$p_2 = 2\varphi p_1 - \varepsilon p$$

$$q_2 = 2\varphi q_1 - \varepsilon q.$$

Hieraus folgt, dafs die Zähler $p, p_1, p_2, \ldots$ eine rekurrente Reihe bilden, deren Beziehungsskala $2\varphi, -\varepsilon$ ist. Dasselbe ist der Fall bei der Reihe der Nenner $q, q_1, q_2, \ldots$ Dieses Resultat gilt nicht nur für die drei ersten Glieder $\frac{p}{q}, \frac{p_1}{q_1}, \frac{p_2}{q_2}$, sondern auch für drei beliebige andere, wofern dieselben unmittelbar aufeinanderfolgen.

Nun ergiebt sich aus der bekannten Theorie dieser Reihen, dafs, wenn man

$$(\varphi + \psi\sqrt{A})^n = \Phi + \Psi\sqrt{A}$$

setzt, wo n eine beliebige ganze Zahl ist, das verlangte allgemeine Glied $\frac{p_n}{q_n}$ durch die Formeln gegeben wird:

$$p_n = a'\Phi + b'\Psi$$

$$q_n = a''\Phi + b''\Psi,$$

worin nur noch die Koefficienten a', b', a'', b'' zu bestimmen sind. Setzt man hierzu $n = 0$ und folglich $\Phi = 1$, $\Psi = 0$, so kann man $p_n = p$, $q_n = q$ setzen, und erhält dadurch:

$$a' = p, \; a'' = q.$$

Ist sodann $n = 1$, so mufs sein:

$$p_1 = p\varphi + b'\psi$$

$$q_1 = q\varphi + b''\psi.$$

Hieraus und aus den bekannten Werten von p_1 und q_1 folgt:

$$b' = -\frac{1}{2}gp - hq$$

$$b'' = \frac{1}{2}gq + fp.$$

Mithin wird schliefslich das **allgemeine Glied** $\frac{p_n}{q_n}$ durch die Formeln bestimmt:

$$p_n = p\Phi - \left(\frac{1}{2}gp + hq\right)\Psi$$

$$q_n = q\Phi + \left(\frac{1}{2}gq + fp\right)\Psi.$$

Wir werden jetzt zeigen, dafs, obwohl die Werte von φ und ψ und folglich auch die von Φ und Ψ dem Anschein nach unter Bruchform sich darstellen, nichtsdestoweniger diese Zahlgröfsen höchstens nur den Bruch $\frac{1}{2}$ enthalten können, was jedoch nicht hindert, dafs die Werte von p_n und q_n stets **ganze** Zahlen sind.

63.

Wir betrachten den Kettenbruch, welcher aus dem vollständigen Quotienten

$$z = \frac{\sqrt{A} + J}{D}$$

hervorgeht, und der sich, wie bereits erwähnt, aus der unendlich oftmal wiederholten Periode $\mu, \mu', \mu'', \ldots \omega$ zusammensetzt. Berechnet man die Näherungsbrüche von z nach der gewöhnlichen Vorschrift:

Quotienten:	μ,	μ',	μ'' ...	ω,	μ,	μ',	μ'', ... ω, ...	
Näherungsbrüche:	$\frac{1}{0}$,	$\frac{\mu}{1}$,	. ...	$\frac{\alpha^0}{\beta^0}$,	$\frac{\alpha}{\beta}$,	. . . .,		

so erhält man nach der ersten Periode:

$$z = \frac{\alpha z + \alpha^0}{\beta z + \beta^0},$$

oder:

$$\beta z^2 + (\beta^0 - \alpha) z = \alpha^0.$$

Setzt man für z seinen Wert $\frac{\sqrt{A} + J}{D}$ ein und setzt sodann die gleichartigen Glieder einander gleich, so ergeben sich die beiden Gleichungen:

$$\beta\left(\frac{A + J^2}{D^2}\right) + (\beta^0 - \alpha)\frac{J}{D} = \alpha^0$$

$$\beta \cdot \frac{2J}{D^2} + \frac{\beta^0 - \alpha}{D} = 0.$$

Hieraus folgt:

$$\frac{\beta J}{D} = -\frac{\beta^0 - \alpha}{2}$$
$$\alpha^0 = \beta\left(\frac{A - J^2}{D^2}\right) = \frac{\beta D^0}{D}.$$

Nun geben die Werte von φ und ψ:

$$\varphi^2 - A\psi^2 = \alpha^2 - \frac{2\alpha\beta}{D}J + \frac{\beta^2}{D^2}J^2 - \frac{\beta^2}{D^2}A,$$

und hierin reduciert sich zunächst wegen $A - J^2 = DD^0$ die rechte Seite auf:

$$\alpha^2 - \frac{2\alpha\beta}{D}J - \frac{\beta^2}{D}D^0.$$

Setzt man sodann die gefundenen Werte von $\frac{\beta J}{D}$ und $\frac{\beta D^0}{D}$ ein, so geht sie über in:

$$\alpha^2 - 2\alpha\left(\frac{\alpha - \beta^0}{2}\right) - \beta\alpha^0,$$

oder in:

$$\alpha\beta^0 - \alpha^0\beta = \pm 1,$$

so dafs man erhält:

$$\varphi^2 - A\psi^2 = \pm 1.$$

Nach diesem Resultate scheint es, als ob die Gröfsen φ und ψ dieselben blieben, mag man die Periode $\mu, \mu', \mu'', \ldots \omega$ mit dem Quotienten μ oder mit jedem andern Gliede $\mu', \mu'', \ldots$ beginnen, wofern dieselbe nur aus denselben Quotienten besteht und letztere in derselben Reihenfolge wie in der Periode geordnet sind. Hierüber kann man sich übrigens leicht Gewifsheit verschaffen, indem man J' und D' an Stelle von J und D nimmt und einen Wert von $\frac{\alpha}{\beta}$ berechnet, welcher den Quotienten $\mu', \mu'' \ldots \omega, \mu$ entspricht. Man wird in der That genau dieselben Werte für die Zahlen φ und ψ erhalten.

Da ferner $\varphi = \alpha - \frac{\beta}{D}J = \frac{\alpha + \beta^0}{2}$ ist, so ist klar, dafs φ eine ganze Zahl ist oder höchstens den Bruch $\frac{1}{2}$ enthält. Von der andern Zahl $\psi = \frac{\beta}{D}$ aber behaupte ich, dafs sie stets eine ganze Zahl ist.

64.

Wäre nämlich $\frac{\beta}{D}$ keine ganze Zahl, so sei $\frac{\gamma}{\delta}$ der einfachste Ausdruck für sie, so dafs man erhielte:

$$\beta = \vartheta\gamma, \quad D = \vartheta\delta.$$

Nun hatten wir gefunden:

$$\frac{\alpha^0}{D^0} = \frac{\beta}{D} = \frac{\gamma}{\delta};$$

man könnte also auch setzen:

$$\alpha^0 = \lambda\gamma, \quad D^0 = \lambda\delta.$$

Ferner ist:

$$\frac{\beta J}{D} = \frac{\gamma J}{\delta} = \frac{\alpha - \beta^0}{2};$$

folglich mufs $\frac{\alpha - \beta^0}{\gamma}$ eine ganze Zahl sein, und demnach kann man setzen:

$$J = \frac{H\delta}{2}.$$

Werden diese Werte in die Gleichung $DD^0 + J^2 = A$ eingesetzt, so erhält man:

$$(4\vartheta\lambda + H^2)\,\delta^2 = 4A = g^2 - 4fh.$$

Wenn also die Zahl $g^2 - 4fh$ keinen quadratischen Teiler hat, so ist notwendig $\delta = 1$, und alsdann ist bewiesen, dafs $\frac{\beta}{D}$ eine ganze Zahl ist. Besitzt dagegen $g^2 - 4fh$ einen quadratischen Faktor δ^2, so kann die vorhergehende Gleichung stattfinden, und wir müssen demnach die weiteren Folgerungen untersuchen, die man aus ihr ziehen kann.

Nun hat man:

$$J = \mu^0 D^0 - J^0, \quad \text{oder } J^0 = \mu^0 D^0 - J = \mu^0 \lambda\delta - \frac{H\delta}{2}.$$

Folglich ist J^0 durch δ teilbar. Man hat ferner:

$$D = D^{00} + \mu^0 (J^0 - J),$$

und hieraus ergiebt sich:

$$D^{00} = D - \mu^0 (J^0 - J).$$

Da die rechte Seite ebenfalls durch δ teilbar ist, so mufs es auch die linke D^{00} und ebenso J^{00}, dessen Wert $\mu^{00} D^{00} - J^0$ ist, sein. Man sieht hieraus, dafs nicht nur die drei Glieder des vollständigen Quotienten $\frac{\sqrt{A} + J}{D}$ durch δ teilbar sind, sondern dafs dasselbe der Fall bei den drei Gliedern eines jeden der vorhergehenden vollständigen Quotienten $\frac{\sqrt{A} + J^0}{D^0}$, $\frac{\sqrt{A} + J^{00}}{D^{00}}$ u. s. w. Geht man also bis auf den ursprünglichen Wert von x zurück, so sieht man, dafs δ nur ein Faktor sein kann, der ohne irgend welchen Zweck in den drei Gliedern der Gröfse $\frac{-\frac{1}{2}g + \sqrt{A}}{f}$ enthalten ist, und da man voraussetzen

kann, dafs ein solcher Faktor nicht existiert, oder dafs derselbe durch Division fortgeschafft sei, so mufs notwendigerweise $\delta = 1$ sein. Mithin ist $\frac{\beta}{D}$ oder ψ stets eine ganze Zahl.

65.

Ist g eine gerade Zahl, so ist A ebenso wie J eine ganze Zahl; alsdann mufs aber auch φ eine ganze Zahl sein, da $\varphi^2 - A\psi^2 = \pm 1$ ist. Ist g dagegen ungerade, so sind A und J Brüche, welche resp. 4 und 2 zu Nennern haben. Jedoch kann es auch in diesem Falle geschehen, dafs ψ eine gerade Zahl wird; alsdann ist φ ebenfalls eine ganze Zahl zufolge der Gleichung $\varphi^2 - A\psi^2 = \pm 1$.

Sind endlich g und ψ gleichzeitig ungerade, so enthält φ den Bruch $\frac{1}{2}$ und setzt man:

$$\varphi = \frac{1}{2}\,\omega, \quad \sqrt{A} = \frac{1}{2}\sqrt{a},$$

so wird:

$$\varphi + \psi\sqrt{A} = \frac{1}{2}\,\omega + \frac{1}{2}\,\psi\sqrt{a}.$$

Ich behaupte nun, dafs eine beliebige ganze Potenz von

$$\frac{1}{2}\,\omega + \frac{1}{2}\,\psi\sqrt{a}$$

höchstens den Bruch $\frac{1}{2}$ enthalten kann. Wegen $\omega^2 - a\psi^2 = \pm 4$ hat man nämlich:

$$\left(\frac{1}{2}\,\omega + \frac{1}{2}\,\psi\sqrt{a}\right)^2 = \frac{1}{2}\,\omega^2 \mp 1 + \frac{1}{2}\,\omega\psi\sqrt{a}$$

$$\left(\frac{1}{2}\,\omega + \frac{1}{2}\,\psi\sqrt{a}\right)^3 = \frac{\omega^3 \mp 3\omega}{2} + \frac{\psi(\omega^2 \mp 1)}{2}\sqrt{a}.$$

Hieraus erkennt man, dafs die zweite Potenz nur allein den Bruch $\frac{1}{2}$, die dritte Potenz aber gar keinen Bruch enthält, da ω ungerade ist, und somit $\frac{\omega^3 \mp 3\omega}{2}$ und $\frac{\omega^2 \mp 1}{2}$ ganze Zahlen werden müssen. Nun ist der Exponent n, welchen Wert er auch haben möge, stets von einer der Formen: $3k$, $3k + 1$, $3k + 2$; mithin kann, da die $3k^{\text{te}}$ Potenz keinen Bruch enthält, die n^{te} Potenz höchstens den Bruch $\frac{1}{2}$ enthalten. Ferner kann diese Potenz durch

$$\Phi + \Psi\sqrt{A} \text{ oder } \Phi + \frac{1}{2}\,\Psi\sqrt{a}$$

dargestellt werden; folglich werden 2Φ und Ψ stets ganze Zahlen sein. Zwischen diesen ganzen Zahlen besteht die Relation:

$$4\Phi^2 - 4A\Psi^2 = \pm 4.$$

66.

Wir kehren zurück zur Betrachtung der Brüche $\frac{p}{q}, \frac{p_1}{q_1}, \frac{p_2}{q_2}, \cdots,$ welche in den aufeinanderfolgenden Perioden einem und demselben vollständigen Quotienten $\frac{\sqrt{A}+J}{D}$ entsprechen. Bezeichnen wir mit $\frac{P}{Q}$ den allgemeinen Ausdruck dieser Brüche (derselbe war oben mit $\frac{p_n}{q_n}$ bezeichnet), so mufs sein:

$$fP^2 + gPQ + hQ^2 = \pm D,$$

wobei das Zeichen + gilt, wenn der Bruch $\frac{P}{Q}$ unter den Näherungsbrüchen von ungerader Ordnung ist, das Zeichen — dagegen, wenn er von gerader Ordnung ist.

Substituiert man nun in die linke Seite die für P und Q gefundenen Werte, nämlich:

$$P = p\Phi - \left(\frac{1}{2}gp + hq\right)\Psi$$

$$Q = q\Phi + \left(\frac{1}{2}gq + fp\right)\Psi,$$

so findet man:

$$fP^2 + gPQ + hQ^2 = (fp^2 + gpq + hq^2)(\Phi^2 - A\Psi^2).$$

Mithin mufs sich, da schon

$$fp^2 + gpq + hq^2 = \pm D$$

war, $\Phi^2 - A\Psi^2$ auf ± 1 reducieren, und dies steht im Einklang mit dem bereits Bewiesenen (No. 63).

Dieser nachträgliche Beweis der Richtigkeit unserer Formel giebt uns ferner zu einer sehr wichtigen Bemerkung Anlafs, nämlich dafs man in den Werten von P und Q das Zeichen von Ψ ändern kann, und dafs die dadurch entstehenden neuen Werte von P und Q ebenfalls der Gleichung

$$fP^2 + gPQ + hQ^2 = \pm D$$

genügen. Untersucht man nun diese zweiten Werte

$$P = p\Phi + \left(\frac{1}{2}gp + hq\right)\Psi$$

$$Q = q\Phi - \left(\frac{1}{2}gq + fp\right)\Psi$$

näher und vergleicht sie mit den ersten, in denen Ψ das entgegengesetzte Zeichen hat, so findet man, dafs dieselben nicht in diesen letzteren enthalten sind, oder wenigstens dafs sie nur dann darin enthalten

sind, wenn man den Exponenten n negativ annimmt (wir werden dies später näher entwickeln). Es müssen daher diese neuen Werte von P und Q notwendigerweise aus der Entwicklung der **zweiten** Wurzel derselben Gleichung $fx^2 + gx + h = 0$ entspringen.

67.

Mithin braucht man nur, um die gegebene Gleichung

$$fy^2 + gyz + hz^2 = \pm D,$$

falls D nicht gröfser ist als $\sqrt{\frac{1}{4}g^2 - fh}$, aufzulösen, eine einzige Wurzel der Gleichung

$$fx^2 + gx + h = 0$$

in einen Kettenbruch zu entwickeln. Die Lösung, welche man mit Hülfe der dem vollständigen Quotienten $\frac{\sqrt{A} + J}{D}$ entsprechenden Näherungsbrüche erhält, wird dann gleichfalls durch blofse Zeichenänderung diejenige Lösung in sich schliefsen, welche aus der Entwicklung der anderen Wurzel entstehen würde. Diese beiden Lösungen sind in die allgemeinen Formeln zusammengefafst:

$$y = p\Phi \pm \left(\frac{1}{2}gp + hq\right)\Psi$$

$$z = q\Phi \mp \left(\frac{1}{2}gq + fp\right)\Psi.$$

Tritt der Fall ein, dafs die gegebene Zahl D sich nicht unter den Nennern der vollständigen Quotienten in der Entwicklung der einen Wurzel findet, so ist es überflüssig, dieselbe Zahl in der Entwicklung der andern Wurzel zu suchen, und man kann dann sicher sein, dafs die in Rede stehende Gleichung nicht in ganzen Zahlen auflösbar ist.

Um jede Schwierigkeit hinsichtlich der Vorzeichen bei der Anwendung der vorhergehenden Formeln zu vermeiden, wollen wir

$$pq^0 - p^0q = i$$

setzen, wo i je nach den verschiedenen Fällen $+1$ oder -1 sein kann. Dann ist zunächst:

$$fp^2 + gpq + hq^2 = iD.$$

Sodann mufs man auf die Anzahl der Glieder der Periode $\mu, \mu', \ldots \omega$ achten. Ist diese Anzahl **gerade**, so werden die verschiedenen Näherungsbrüche $\frac{p}{q}, \frac{p_1}{q_1}, \frac{p_2}{q_2}, \cdots$ gleichartige Stellen

einnehmen, d. h. sie werden entweder sämtlich von gerader Ordnung oder sämtlich von ungerader Ordnung sein. Folglich wird die Gleichung

$$fy^2 + gyz + hz^2 = iD$$

aufgelöst durch die Formeln:

$$y = p\Phi \pm \left(\frac{1}{2} gp + hq\right)\Psi$$

$$z = q\Phi \mp \left(\frac{1}{2} gq + fp\right)\Psi,$$

wobei

$$(\varphi + \psi\sqrt{A})^n = \Phi + \Psi\sqrt{A}$$

ist.

In diesem Falle läfst sich die Gleichung

$$fy^2 + gyz + hz^2 = - iD$$

nicht in ganzen Zahlen auflösen, jedenfalls nicht mittelst des Näherungsbruches $\frac{p}{q}$.

Ist dagegen die Anzahl der Glieder der Periode **ungerade**, so kann man mittelst eben derselben Formeln gleichzeitig die Gleichung

$$fy^2 + gyz + hz^2 = + iD$$

und die Gleichung

$$fy^2 + gyz + hz^2 = - iD$$

auflösen, und zwar erstere, indem man $n = 2k$, letztere, indem man $n = 2k + 1$ setzt.

68.

Da der Fall $D = 1$ sehr häufige Anwendung finden wird, so wird es angemessen sein, ihn besonders zu untersuchen. Man hat alsdann (No. 62):

$$\frac{q^0}{q} + J = \frac{1}{2} g + f \frac{p}{q}.$$

Nun ist aber $\frac{1}{2} g + f \cdot \frac{p}{q}$ ein sehr nahe bei $\sqrt{A}$ oder $\frac{1}{2}\sqrt{g^2 - 4fh}$ liegender Wert. Bezeichnet man daher, im Falle g ungerade ist, mit m die gröfste in $\sqrt{g^2 - 4fh}$ enthaltene ungerade Zahl, und im Falle g gerade ist, mit m die gröfste in eben dieser Quadratwurzel enthaltene gerade Zahl, so erhält man (da $\frac{q^0}{q}$ kleiner als 1 ist) in beiden Fällen:

$$J = \frac{m}{2}.$$

Zu gleicher Zeit geht der vollständige Quotient $\frac{\sqrt{A}+J}{D}$ über in $\sqrt{A}+\frac{m}{2}$, und daher ist die gröſste darin enthaltene ganze Zahl $\mu = m$. Dies ist der Wert des Quotienten, welcher in den aufeinanderfolgenden Perioden dem Werte $D = 1$ entspricht.

Ist stets $\mu, \mu', \mu'', \ldots \omega$ die Periode der Quotienten und $\frac{\alpha}{\beta}$ der daraus entstehende Bruch, so haben wir oben gefunden:

$$\frac{2\beta J}{D} = \alpha - \beta^0.$$

Wenn also $D = 1$ und $J = \frac{m}{2}$ ist, so erhält man:

$$\beta^0 = \alpha - m\beta = \alpha - \mu\beta.$$

Man erkennt hieraus, daſs die Quotienten $\mu', \mu'', \ldots \omega$ eine symmetrische Reihe bilden (No. 32), und demnach ist die sich unendlich oft wiederholende Periode von der Form $m, \mu', \mu'', \ldots \mu'', \mu'$. Endlich ergiebt sich in dem nämlichen Falle $\varphi = \alpha - \frac{1}{2}m\beta$, $\psi = \beta$.

69.

Die allgemeinen Formeln lassen sich, falls g eine **gerade** Zahl ist, mag die Zahl D sein, welche sie wolle, vereinfachen und von den Brüchen befreien. Soll dann die Gleichung:

$$ay^2 + 2byz + cz^2 = \pm D,$$

welche

$$f = a, \quad g = 2b, \quad h = c, \quad A = b^2 - ac$$

giebt, aufgelöst werden, so bezeichne man, wie immer, mit $\mu, \mu', \mu'', \ldots \omega$ die Periode, welche unendlich oft wiederholt die Entwicklung des vollständigen Quotienten $\frac{\sqrt{A}+J}{D}$ bildet, und berechne mit Hülfe dieser Periode den Bruch $\frac{\alpha}{\beta}$, wie folgt:

Quotienten: $\mu\,,\ \mu', \mu'', \cdots \omega$

Näherungsbrüche: $\frac{1}{0}, \ \frac{\mu}{1} \cdots\cdots \frac{\alpha^0}{\beta^0}, \ \frac{\alpha}{\beta}$.

Alsdann erhält man:

$$\varphi = \frac{\alpha + \beta^0}{2} = \alpha - \frac{\beta}{D}J$$

$$\psi = \frac{\beta}{D},$$

und diese Werte werden stets ganze Zahlen sein. Setzt man sodann:

$$(\varphi + \psi\sqrt{A})^n = \Phi + \Psi\sqrt{A}$$
$$y = p\Phi \pm (bp + cq)\Psi$$
$$z = q\Phi \mp (bq + ap)\Psi,$$

so ergiebt sich:

$$ay^2 + 2byz + cz^2 = \pm D,$$

und was das doppelte Vorzeichen anlangt, so wird dasselbe bestimmt durch die Formel:

$$ay^2 + 2byz + cz^2 = (\varphi^2 - A\psi^2)^n (pq^0 - p^0 q) D,$$

worin bekanntlich $\varphi^2 - A\psi^2$ ebenso wie $pq^0 - p^0 q$ nur entweder gleich $+1$ oder gleich -1 sein kann.

Die Zahlen φ und ψ, die man in der eben angegebenen Weise durch Berechnung einer Periode gefunden hat, sind stets die einfachsten von allen denen, welche der Gleichung $\varphi^2 - A\psi^2 = \pm 1$ genügen. Denn wären sie es nicht, so müfste man annehmen, entweder dafs die betreffende Periode aus mehreren kürzeren Perioden zusammengesetzt ist, oder dafs es Lösungen der gegebenen Gleichung giebt, die nicht unter den Näherungsbrüchen enthalten sind. Der erste Fall kann wegen unserer Voraussetzung nicht stattfinden, und der zweite ist unmöglich, wie im § 12 bewiesen werden wird. Mithin hängen die Zahlen Φ und Ψ nur von der einen Zahl A ab.

Es ist überflüssig hinzuzufügen, dafs, wenn die Zahl D sich mehrere Mal innerhalb einer Periode vorfindet, daraus eine gleiche Anzahl verschiedener Lösungen der gegebenen Gleichung abgeleitet werden kann.

§ 10.

Vergleichung der aus der Entwicklung der beiden Wurzeln einer und derselben Gleichung zweiten Grades hervorgehenden Kettenbrüche.

70.

Wir haben bereits bemerkt (No. 66), dafs die beiden Wurzeln einer und derselben Gleichung zweiten Grades

$$fx^2 + gx + h = 0,$$

in einen Kettenbruch verwandelt, in gleicher Weise zur Auflösung der Gleichung

$$fy^2 + gyz + hz^2 = \pm D$$

beitragen, so dafs sich in den beiden Reihen vollständiger Quotienten, welche aus der Entwicklung dieser Wurzeln entspringen, notwendigerweise dieselben Werte von D vorfinden müssen. Wir wollen jetzt diese Eigenschaft in ihr volles Licht setzen und allgemein zeigen,

dafs, wenn die Reihe der vollständigen Quotienten, nachdem sie regulär geworden, in der Entwicklung der einen Wurzel folgendermafsen fortschreitet:

$$\frac{\sqrt{A}+J^0}{D^0}=\mu^0+$$

$$\frac{\sqrt{A}+J}{D}=\mu+$$

$$\frac{\sqrt{A}+J'}{D'}=\mu'+$$

u. s. w.,

die Entwicklung der zweiten Wurzel, wenigstens nach einigen am Anfang abweichenden Gliedern, diese andere Reihe in umgekehrter Reihenfolge liefern wird:

$$\frac{\sqrt{A}+J'}{D}=\mu+$$

$$\frac{\sqrt{A}+J}{D^0}=\mu^0+$$

$$\frac{\sqrt{A}+J^0}{D^{00}}=\mu^{00}+$$

u. s. w.,

welche notwendig auf das erste Glied $\frac{\sqrt{A}+J'}{D}$ zurückkommt und bis ins Unendliche immer von neuem wieder ebenso beginnt.

Wir betrachten wiederum die Kettenbruchentwicklung der Wurzel

$$x=\frac{\sqrt{A}-\frac{1}{2}g}{f},$$

und bezeichnen mit $\frac{p^0}{q^0}$, $\frac{p}{q}$, $\frac{p'}{q'}$ drei aufeinanderfolgende Näherungsbrüche, welche aus der ersten Periode der Quotienten*), nachdem jede Unregelmäfsigkeit aufgehört, und man sich überzeugt hat, dafs diese nämliche Periode sich bis ins Unendliche immer wiederholen mufs, entnommen sind. Wie gewöhnlich, stellen wir die drei entsprechenden vollständigen Quotienten durch $\frac{\sqrt{A}+J^0}{D^0}$, $\frac{\sqrt{A}+J}{D}$, $\frac{\sqrt{A}+J'}{D'}$ und die gröfsten in ihnen enthaltenen ganzen Zahlen durch μ^0, μ, μ' dar. Was die Periode der Quotienten angeht, so ist die-

*) Diese Periode könnte weniger als drei Glieder enthalten; alsdann aber würde man, um für diesen besonderen Fall keine Ausnahme zu machen, mehrere Perioden zusammenfassen. Anm. d. Verf.

selbe μ, μ', μ'', ... μ^0, wenn man sie mit dem Gliede μ beginnen läfst; sie würde in gleicher Weise μ', μ'', ... μ^0, μ sein, wenn man sie mit dem Gliede μ' beginnen liefse, und so je nach Belieben; allgemein kann man die betreffende Periode anfangen lassen, bei welchem Gliede man will, sie mufs jedoch aus denselben Gliedern in derselben Reihenfolge bestehen.

Sucht man nun die verschiedenen Näherungsbrüche $\frac{p}{q}, \frac{p_1}{q_1}, \frac{p_2}{q_2}, \cdots$, welche in den aufeinanderfolgenden Perioden dieselbe Stelle einnehmen, oder welche demselben vollständigen Quotienten $\frac{\sqrt{A}+J}{D}$ entsprechen, so wird, wie wir in No. 62 gesehen haben, der allgemeine Ausdruck dieser Brüche $\frac{p_n}{q_n}$ durch die Formeln gegeben:

$$\begin{aligned} p_n &= p\Phi - \left(\frac{1}{2}gp + hq\right)\Psi \\ q_n &= q\Phi + \left(\frac{1}{2}gq + fp\right)\Psi, \end{aligned} \qquad (a)$$

wobei

$$\Phi + \Psi\sqrt{A} = (\varphi + \psi\sqrt{A})^n$$

und

$$\Phi^2 - A\Psi^2 = (\varphi^2 - A\psi^2)^n = (\pm 1)^n$$

ist.

Man hat also nur n der Reihe nach die Werte 0, 1, 2, 3, ... zu geben und die sich dadurch ergebenden Werte von Φ und Ψ einzusetzen, um nach und nach alle in Rede stehenden Näherungsbrüche $\frac{p}{q}, \frac{p_1}{q_1}, \frac{p_2}{q_2} \cdots$ zu erhalten. Es bleibt nur noch zu untersuchen, was geschieht, wenn man n **negative** Werte $-1, -2, -3, \ldots$ giebt.

71

Nun hat man:

$$(\varphi + \psi\sqrt{A})^{-n} = (\varphi^2 - A\psi^2)^{-n}(\varphi - \psi\sqrt{A})^n = (\pm 1)^n(\Phi - \Psi\sqrt{A}).$$

Mithin kommt die Annahme eines negativen n einfach darauf zurück, dafs Ψ sein Zeichen ändert, und dafs die Werte von Φ und Ψ mit einem und demselben Faktor $(\pm 1)^n$ multipliciert werden, wobei diese ambige Gröfse ± 1 von $\varphi^2 - A\psi^2$, welches in der That $+1$ oder -1 sein kann, herrührt. Da jedoch der Bruch $\frac{p_n}{q_n}$ von $\frac{-p_n}{-q_n}$ nicht verschieden ist, so kann man von dem Faktor $(\pm 1)^n$ absehen. Demnach werden negative Werte von n neuen

Werten von $\frac{p_n}{q_n}$ entsprechen, welche durch die Formeln

$$p_n = p\Phi + \left(\frac{1}{2}gp + hq\right)\Psi \qquad (b)$$
$$q_n = q\Phi - \left(\frac{1}{2}gq + fp\right)\Psi$$

gegeben werden. Man könnte zunächst glauben, daſs sich diese Formeln von den ersten nur durch die Form unterscheiden, und daſs sie in Wirklichkeit zu denselben Werten von $\frac{p_n}{q_n}$ führen. Dazu müſsten zwei solche Brüche wie

$$\frac{p\Phi - (\frac{1}{2}gp + hq)\Psi}{q\Phi + (\frac{1}{2}gq + fp)\Psi}, \quad \frac{p\Phi' + (\frac{1}{2}gp + hq)\Psi'}{q\Phi' - (\frac{1}{2}gq + fp)\Psi'}$$

einander gleich sein können. Dies kann jedoch niemals stattfinden; denn bringt man sie auf denselben Nenner, so findet man die Differenz der Zähler gleich $(fp^2 + gpq + hq^2)(\Phi'\Psi + \Phi\Psi')$, eine Gröſse, die niemals 0 sein kann.

Mithin ist sicher, daſs die Formeln (b) Werte von $\frac{p_n}{q_n}$ geben, welche verschieden sind von denen, welche die Formeln (a) liefern. Setzt man aber, sei es in den Formeln (b), sei es in den Formeln (a), $p_n = y$, $q_n = z$, so genügen die allgemeinen Werte von y und z der Gleichung:

$$fy^2 + gyz + hz^2 = \pm D.$$

Andrerseits kann man, da D kleiner als $\sqrt{A}$ vorausgesetzt ist, beweisen, daſs jeder Bruch $\frac{y}{z}$, welcher dieser Gleichung genügt, unter den Näherungsbrüchen einer Wurzel der Gleichung

$$fx^2 + gx + h = 0$$

enthalten ist. Wenn demnach die Formeln (b) Brüche $\frac{p_n}{q_n}$ geben, welche nicht unter den Näherungsbrüchen der Wurzel $x = \frac{\sqrt{A} - \frac{1}{2}g}{f}$ enthalten sind, so müssen eben diese Brüche $\frac{p_n}{q_n}$ unter den Näherungsbrüchen der andern Wurzel $x' = \frac{-\sqrt{A} - \frac{1}{2}g}{f}$ enthalten sein.

Man darf nicht vergessen, daſs unter den Näherungsbrüchen, welche dem vollständigen Quotienten $\frac{\sqrt{A} + J}{D}$ entsprechen, $\frac{p}{q}$ der Annahme nach der einfachste oder derjenige sein soll, welcher in

der ersten Periode enthalten ist. Setzt man in den Formeln (a) $n = -1$, oder in den Formeln (b) $n = 1$, so kann der dadurch entstehende Bruch zu dem irregulären Teile der Entwicklung der einen oder andern Wurzel gehören oder sogar in keiner Entwicklung vorkommen, und zwar aus Gründen, die wir anderwärts auseinandersetzen werden. Setzt man aber in den Formeln (b) $n > 1$, so wird der dadurch entstehende Bruch sicher einer der Näherungsbrüche der Wurzel $x = \frac{-\sqrt{A} - \frac{1}{2}g}{f}$ sein.

72.

Ist also unter der Voraussetzung, dafs $n > 1$ sei,

$$(\varphi + \psi\sqrt{A})^n = \Phi + \Psi\sqrt{A},$$

und:

$$P = p\Phi + \left(\frac{1}{2}gp + hq\right)\Psi$$

$$Q = q\Phi - \left(\frac{1}{2}gq + fp\right)\Psi,$$

so ist $\frac{P}{Q}$ einer der Näherungsbrüche der Wurzel:

$$x' = \frac{-\sqrt{A} - \frac{1}{2}g}{f}.$$

Setzt man aber in analoger Weise:

$$P^0 = -p'\Phi - \left(\frac{1}{2}gp' + hq'\right)\Psi$$

$$Q^0 = -q'\Phi + \left(\frac{1}{2}gq' + fp'\right)\Psi$$

$$P' = -p^0\Phi - \left(\frac{1}{2}gp^0 + hq^0\right)\Psi$$

$$Q' = -q^0\Phi + \left(\frac{1}{2}gq^0 + fp^0\right)\Psi,$$

so sind $\frac{P^0}{Q^0}$, $\frac{P'}{Q'}$ offenbar ebenfalls Näherungsbrüche derselben Wurzel. Es handelt sich jetzt darum, zu zeigen, dafs die drei Näherungsbrüche $\frac{P^0}{Q^0}$, $\frac{P}{Q}$, $\frac{P'}{Q'}$ unmittelbar in der Reihenfolge, wie sie hingeschrieben sind, aufeinanderfolgen.

Zunächst geben die vorhergehenden Werte:

$$PQ^0 - P^0Q = (p'q - pq')(\Phi^2 - A\Psi^2) = \pm 1$$

und:

$$P'Q - PQ' = -(PQ^0 - P^0Q),$$

Bedingungen, die alle beide zu dem Zwecke, den wir im Auge haben, notwendig sind. Indessen sind dieselben noch nicht hinreichend.

Man kann, um eine bestimmte Vorstellung zu haben, annehmen, dafs der Wert von n ein ziemlich grofser ist, so dafs der Näherungsbruch $\frac{P}{Q}$ einer ziemlich weit vom Anfang der Reihe entfernten Periode entspricht. Da alle Perioden gleich sind, so thut es wenig zur Sache, welche Periode wir betrachten; und die Form, die wir für eine entfernte Periode finden, kommt in gleicher Weise allen andern Perioden zu. Ist aber n eine ziemlich grofse Zahl, so sind die Zahlen Φ und Ψ sehr beträchtlich, und da stets $\Phi^2 - A\Psi^2 = (\pm 1)^n = \pm 1$ ist, so folgt daraus, dafs alsdann sehr nahe $\Phi = \Psi\sqrt{A}$ ist. Substituiert man diesen Wert in den Wert von P, so erhält man:

$$P = \Psi\,(p\sqrt{A} + \frac{1}{2}gp + hq) = \Psi\,(\sqrt{A} + \frac{1}{2}g)\,(p - qx),$$

wo x die erste Wurzel $\frac{\sqrt{A} - \frac{1}{2}g}{f}$, von welcher $\frac{p}{q}$ ein Näherungswert ist, bezeichnet.

Ähnliche Werte findet man für P^0 und P', und setzt man zur Abkürzung den konstanten Faktor $\Psi(\sqrt{A} + \frac{1}{2}g) = R$, so erhält man:

$$\begin{aligned} P^0 &= - R(p' - q'x) \\ P &= R(p - qx) \\ P' &= - R(p^0 - q^0x). \end{aligned}$$

Ist z der vollständige Quotient, welcher dem Näherungsbruche $\frac{p}{q}$ in der Entwicklung des Wertes von x entspricht, so ist:

$$x = \frac{pz + p^0}{qz + q^0}$$

oder:

$$z = \frac{-(p^0 - q^0x)}{p - qx}.$$

Nun mufs aber z positiv und gröfser als 1 sein; mithin ist $-(p^0 - q^0x)$ gröfser als $p - qx$ und gleichen Zeichens mit diesem. Aus demselben Grunde ist $p - qx$ gleichen Zeichens mit $-(p' - q'x)$ und gröfser wie dieses. Folglich besitzen die drei Zahlen P^0, P, P' dasselbe Zeichen und folgen der Gröfse nach derart aufeinander, dafs $P^0 < P$, $P < P'$ ist. Dasselbe kann man von den drei Zahlen Q^0, Q, Q' beweisen. Wenn nun, nachdem dieses feststeht, die beiden Näherungsbrüche $\frac{P^0}{Q^0}$, $\frac{P}{Q}$ nicht unmittelbar aufeinanderfolgen, so kann man zwischen ihnen höchstens nur noch den Bruch $\frac{P - P^0}{Q - Q^0}$

annehmen. Denn da bereits $PQ^0 - P^0Q = \pm 1$ ist und da, wenn man den $\frac{P}{Q}$ unmittelbar vorhergehenden Näherungsbruch durch $\frac{M}{N}$ darstellt, auch $PN - MQ = \pm 1$ sein mufs, so ergiebt sich daraus:

$$M = kP \pm P^0, \quad N = kQ \pm Q^0,$$

wo k eine unbestimmte Zahl ist. Nun ergiebt aber die Bedingung, dafs M zwischen P und P^0 enthalten sein solle, $k = 1$, und:

$$M = P - P^0, \quad N = Q - Q^0.$$

Mithin kann man sicher sein, dafs dem Näherungsbruche $\frac{P}{Q}$ der Bruch $\frac{P^0}{Q^0}$ oder wenigstens der Bruch $\frac{P - P^0}{Q - Q^0}$ vorhergeht.

73.

Diese Ungewifsheit wird bald aufgeklärt sein, wenn wir den vollständigen Quotienten, welcher dem Bruche $\frac{P}{Q}$ entspricht, bestimmen. Ist z dieser vollständige Quotient unter der Annahme, dafs $\frac{P^0}{Q^0}$ unmittelbar $\frac{P}{Q}$ vorhergeht, so würde der vollständige Wert des Kettenbruches

$$\frac{Pz + P^0}{Qz + Q^0}$$

sein. Ist dagegen y der vollständige Quotient unter der Annahme, dafs $\frac{P - P^0}{Q - Q^0}$ unmittelbar $\frac{P}{Q}$ vorausgeht, so würde man als vollständigen Wert des Kettenbruches erhalten:

$$\frac{Py + P - P^0}{Qy + Q - Q^0} = \frac{-P(y+1) + P^0}{-Q(y+1) + Q^0}.$$

Nun ist offenbar diese zweite Annahme in der ersten enthalten, wenn man $z = -(y + 1)$ setzt. Geht man demnach von der ersten Annahme aus, und findet man einen positiven Wert von z, so ist dies ein Beweis dafür, dafs diese Annahme die richtige ist, und dafs in der That $\frac{P^0}{Q^0}$, $\frac{P}{Q}$ aufeinanderfolgende Näherungsbrüche sind. Giebt dagegen die Rechnung einen negativen Wert für z, so folgt daraus die Richtigkeit der zweiten Annahme.

Ich behaupte nun, dafs der Wert von z nicht allein positiv, sondern auch im Allgemeinen $\frac{\sqrt{A} + J'}{D}$ ist, und ferner, dafs die gröfste in diesem Ausdrucke enthaltene ganze Zahl μ ist. Ist das letztere richtig, so mufs man also haben:

$$P' = \mu P + P^0, \quad Q' = \mu Q + Q^0,$$

und dies bestätigt sich unmittelbar mit Hülfe der Werte von P, Q, P^0, Q^0 u. s. w., da stets $p' = \mu p + p^0$, $q' = \mu q + q^0$. Der zweite Teil kann übrigens auch allgemein folgendermafsen bewiesen werden.

Zunächst ist:

$$J' = \mu D - J.$$

Dies giebt:

$$\frac{\sqrt{A} + J'}{D} = \mu + \frac{\sqrt{A} - J}{D}.$$

Ferner folgt aus dem in No. 62 für q^0 gefundenen Werte:

$$\frac{q^0}{q} = \frac{\frac{1}{2}g - J}{D} + \frac{f}{D} \cdot \frac{p}{q},$$

und da $\frac{p}{q}$ bereits ein sehr angenäherter Wert von $\frac{\sqrt{A} - \frac{1}{2}g}{f}$ ist, so hat man ziemlich nahe:

$$\frac{q^0}{q} = \frac{\frac{1}{2}g - J}{D} + \frac{f}{D} \cdot \frac{\sqrt{A} - \frac{1}{2}g}{f} = \frac{\sqrt{A} - J}{D}.$$

Daraus ersieht man, dafs $\frac{\sqrt{A} - J}{D}$, welches sehr nahe gleich $\frac{q^0}{q}$ ist, stets kleiner als die Einheit ist; mithin erhält man in unserer gewohnten Bezeichnung:

$$\frac{\sqrt{A} + J'}{D} = \mu +$$

Wir kommen jetzt zum ersten Teile unserer Behauptung. Ist $\frac{\sqrt{A} + J'}{D}$ der vollständige Quotient, welcher dem Näherungsbruche $\frac{P}{Q}$ entspricht, und folgt letzterer unmittelbar auf $\frac{P^0}{Q^0}$, so mufs der Wert der zweiten Wurzel x' der Gleichung $fx^2 + gx + h = 0$ gleich

$$x' = \frac{P(\sqrt{A} + J') + P^0 D}{Q(\sqrt{A} + J') + Q^0 D}$$

sein. Setzt man für J' seinen Wert $\mu D - J$, und beachtet man, dafs

$$\mu P + P^0 = P', \quad \mu Q + Q^0 = Q'$$

ist, so geht diese Gleichung über in:

$$x' = \frac{P(\sqrt{A} - J) + P' D}{Q(\sqrt{A} - J) + Q' D}.$$

Substituiert man hierin ferner für P, Q, P', Q' ihre Werte und setzt sodann im Resultat die in No. 62 für p^0 und q^0 gefundenen Werte ein, so folgt:

$$x' = \frac{\Phi(p\sqrt{A} + \frac{1}{2}gp + hq) + \Psi(\frac{1}{2}gp\sqrt{A} + hq\sqrt{A} + Ap)}{\Phi(q\sqrt{A} - \frac{1}{2}gq - fp) - \Psi(\frac{1}{2}gq\sqrt{A} + fp\sqrt{A} - Aq)},$$

und dieser Ausdruck läfst sich auf die Form bringen:

$$x' = \frac{(\Phi + \Psi\sqrt{A})\,(p\sqrt{A} + \frac{1}{2}gp + hq)}{(\Phi + \Psi\sqrt{A})\,(q\sqrt{A} - \frac{1}{2}gq - fp)}.$$

Unterdrückt man also den gemeinsamen Faktor im Zähler und Nenner, so erhält man:

$$x' = \frac{p\sqrt{A} + \frac{1}{2}gp + hq}{q\sqrt{A} - \frac{1}{2}gq - fp}.$$

Wegen $A = \frac{1}{4}g^2 - fh$ ist aber:

$$h = \frac{(\frac{1}{2}g + \sqrt{A})\,(\frac{1}{2}g - \sqrt{A})}{f},$$

und daher:

$$p\sqrt{A} + \frac{1}{2}gp + hq = \frac{\sqrt{A} + \frac{1}{2}g}{f}\,(fp + \frac{1}{2}gq - q\sqrt{A}).$$

Mithin reduciert sich schliefslich der Wert von x' auf:

$$x' = \frac{-\sqrt{A} - \frac{1}{2}g}{f},$$

und dieses ist die zweite Wurzel der Gleichung $fx^2 + gx + h = 0$.

74.

Dieses Resultat bestätigt vollkommen die verschiedenen, von uns aufgestellten Behauptungen. Als hauptsächliche Folgerung ergiebt sich daraus, dafs $\frac{\sqrt{A} + J'}{D}$ der vollständige Quotient ist, welcher in der Entwicklung der zweiten Wurzel x' dem Näherungsbruche $\frac{P}{Q}$ entspricht. Aus demselben Grunde ist der dem folgenden Bruche $\frac{P'}{Q'}$ entsprechende vollständige Quotient $\frac{\sqrt{A} + J}{D^0}$, und der, welcher unmittelbar darauf kommt, $\frac{\sqrt{A} + J^0}{D^{00}}$ u. s. w. Man erkennt daraus, dafs die Nenner D, D^0, $D^{00}, \ldots$ in umgekehrter Reihenfolge, wie diejenige ist, in der sie in der Entwicklung der ersten Wurzel vorkommen, aufeinanderfolgen.

Übrigens genügt die Existenz des vollständigen Quotienten $\frac{\sqrt{A}+J'}{D}$, um die der folgenden Quotienten zu beweisen, und zwar erhält man letztere durch das gewöhnliche Verfahren der Entwicklung in einen Kettenbruch. Denn wie wir bereits gesehen haben, ist die gröfste in $\frac{\sqrt{A} + J'}{D}$ enthaltene ganze Zahl μ. Hieraus und aus den bereits durch

die Entwicklung der ersten Wurzel bekannten Relationen leitet man die Reihe ab:

$$\frac{\sqrt{A} + J'}{D} = \mu + \frac{\sqrt{A} - J}{D}$$

$$\frac{D}{\sqrt{A} - J} = \frac{\sqrt{A} + J}{D^0} = \mu^0 + \frac{\sqrt{A} - J^0}{D^0}$$

$$\frac{D^0}{\sqrt{A} - J^0} = \frac{\sqrt{A} + J^0}{D^{00}} = \mu^{00} + \frac{\sqrt{A} - J^{00}}{D^{00}}$$

u. s. w.

Die Reihe der Quotienten μ, μ^0, $\mu^{00}, \ldots$ mufs notwendig wieder auf den Quotienten μ zurückkommen; mithin besteht die Periode, welche in der Entwicklung der zweiten Wurzel auftritt, aus denselben Gliedern, wie die Periode der ersten Wurzel, nur mit dem einen Unterschiede, dafs die Glieder in der umgekehrten Reihenfolge geordnet sind.

Wenn der Fall einträte, dafs die in der Entwicklung der einen Wurzel vorkommende Periode von der Form $\mu, \mu', \mu'', \ldots \mu'', \mu', \mu, k$ wäre, d. h. aus einem symmetrischen Teile bestände, dem ein einzelnes Glied k vorausgeht oder nachfolgt, so würde die Umkehrung stets dieselbe Periode ergeben, und letztere würde somit den beiden Wurzeln der Gleichung gemeinsam sein. Dies kann man bei einer grofsen Anzahl von Fällen beobachten. Alsdann kommen auch in der Entwicklung der beiden Wurzeln dieselben vollständigen Quotienten vor und folgen in derselben Ordnung aufeinander.

§ 11.
Auflösung der Gleichung $Ly^2 + Myz + Nz^2 = \pm H$ in ganzen Zahlen.

75.

Je nachdem y und z zu einander prim sind oder nicht, mufs man zwei Fälle unterscheiden. Um den zweiten Fall auf den ersten zurückzuführen, bezeichnen wir mit ϑ das gröfste gemeinschaftliche Mafs von y und z, und es sei $y = \vartheta y'$, $z = \vartheta z'$. Da alsdann die linke Seite durch ϑ^2 teilbar ist, mufs auch H durch ϑ^2 teilbar sein. Ist also $H = \vartheta^2 H'$, so erhält man:

$$Ly'^2 + My'z' + Nz'^2 = \pm H',$$

eine Gleichung, in der nunmehr y' und z' prim zu einander sind. So oft es also Quadratzahlen ϑ^2, welche H teilen, giebt, hat man stets der vorhergehenden ähnliche Gleichungen aufzulösen, in denen die unbestimmten Zahlen relative Primzahlen sind.

Man kann voraussetzen, dafs diese Art der Zerlegung durch eine vorbereitende Rechnung bereits ausgeführt ist; mithin können wir die gegebene Gleichung

$$Ly^2 + Myz + Nz^2 = \pm H$$

als eine von denen ansehen, in welchen die unbestimmten Zahlen y und z prim zu einander sein sollen.

Nachdem wir dies vorausgeschickt haben, unterscheiden wir noch den Fall, wo z und H zu einander prim sind, und den, in welchem sie einen gemeinsamen Teiler ϑ haben. Ist in diesem letzteren Falle $z = \vartheta z'$, $H = \vartheta H'$, so mufs $\frac{Ly^2}{\vartheta}$ eine ganze Zahl sein. Da aber y mit z und demnach auch mit ϑ keinen gemeinsamen Teiler hat, so erfordert diese Bedingung, dafs L durch ϑ teilbar sei. Ist daher $L = \vartheta L'$, so geht die aufzulösende Gleichung über in:

$$L'y^2 + Myz' + \vartheta N z'^2 = \pm H',$$

in welcher man nunmehr z' und H' als relative Primzahlen betrachten kann.

So oft es also zwischen L und H gemeinschaftliche Teiler (die Einheit mit einbegriffen) giebt, hat man immer Gleichungen aufzulösen, in denen z' und H' zu einander prim sind. Man kann aber diese vielen aufzulösenden Fälle leicht vermeiden mittelst einer Transformation, welche darin besteht, dafs man $y' + mz$ an die Stelle von y setzt und m derart bestimmt, dafs $Lm^2 + Mm + N$ mit H keinen gemeinsamen Teiler besitzt. Alsdann kann die neue Unbestimmte y' mit H keinen gemeinsamen Teiler mehr haben. Die ganze Schwierigkeit reduciert sich also darauf, die Gleichung

$$Ly^2 + Myz + Nz^2 = \pm H$$

in welcher z und y, ebenso wie z und H zu einander prim sind, aufzulösen. Diese Gleichung bietet aber verschiedene zu untersuchende Fälle dar, je nachdem die Zahl $4LN - M^2$ positiv, Null oder negativ ist, d. h. je nachdem die beiden Faktoren der linken Seite imaginär, gleich oder reell sind.

76.

Es sei zuerst $4LN - M^2$ gleich einer **positiven** Zahl B. Multipliciert man die gegebene Gleichung mit $4L$, und setzt man $2Ly + Mz = x$, so erhält man:

$$x^2 + Bz^2 = + 4LH.$$

(Wir schreiben auf der rechten Seite nur das Zeichen $+$, weil man

leicht erkennt, dafs das Zeichen — nicht stattfinden kann). Die einfachste Methode zur Auflösung der Gleichung $x^2 + Bz^2 = C$ besteht nun darin, dafs man nach und nach die verschiedenen Werte der Zahlgröfse $C - Bz^2$ berechnet, indem man $z = 0, 1, 2, 3, \ldots$ bis $z = \sqrt{\frac{C}{B}}$ setzt. Findet sich unter diesen Werten eine Quadratzahl, und macht zugleich die Wurzel x dieses Quadrats den Ausdruck $\frac{Mz \pm x}{2L}$ zu einer ganzen Zahl, so erhält man eine Lösung der gegebenen Gleichung. Können aber diese beiden Bedingungen nicht zu gleicher Zeit erfüllt werden, so folgt daraus, dafs die gegebene Gleichung nicht in ganzen Zahlen auflösbar ist.

Es ist ersichtlich, dafs es in diesem Falle nur eine beschränkte Anzahl von ganzzahligen Lösungen geben kann. Übrigens ist dieser Fall so einfach, dafs er keiner der im vorhergehenden Artikel angedeuteten Vorbereitungen bedarf, und dafs man zu seiner Auflösung, wie eben angegeben, verfahren kann, ohne sich darum zu kümmern, ob y, z und H einen gemeinschaftlichen Teiler haben oder nicht.

77.

Wir nehmen als Beispiel die Gleichung:

$$15y^2 + 43yz + 32z^2 = 223.$$

Multipliciert man beide Seiten mit 60, und setzt man:

$$30y + 43z = x,$$

so wird die transformierte Gleichung:

$$x^2 + 71z^2 = 13380.$$

Wir berechnen also die Gröfse $13380 - 71z^2$, indem wir der Reihe nach $z = 0, 1, 2, 3, \ldots$ setzen, bis die in Rede stehende Gröfse aufhört positiv zu sein. Die Resultate, die man mit Hülfe ihrer gleichmäfsig wachsenden Differenzen leicht erhält, sind:

Werte von x^2:	13380,	13309,	13096,	12741,	12244,	11605,	10824,
Differenzen:	71,	213,	355,	497,	639,	781,	923,
Werte von x^2:	9901,	8836,	7629,	6280,	4789,	3156,	1381.
Differenzen:	1065,	1207,	1349,	1491,	1633,	1775.	

Nun ist unter diesen Resultaten nur 8836 ein vollständiges Quadrat, nämlich das Quadrat von 94. Mithin sind die einzigen brauchbaren Werte von z und x: $z = 8$ und $x = \pm 94$. Hieraus ergiebt sich aber:

$$y = \frac{\pm 94 - 344}{30},$$

und dieser Wert reduciert sich nicht auf eine ganze Zahl. Die gegebene Gleichung ist demnach nicht in ganzen Zahlen auflösbar; man kann ihr nur durch rationale Werte Genüge leisten, z. B. durch $z = 8$, $y = -\frac{25}{3}$ und unendlich viele andere.

78.

Ist $4LN - M^2 = 0$ oder sind die Faktoren der linken Seite der gegebenen Gleichung einander gleich, so mufs diese Gleichung, wenn sie auflösbar sein soll, die Form $(my + nz)^2 = h^2$ haben. Alsdann reduciert sie sich auf die Gleichung ersten Grades $my + nz = \pm h$, welche immer möglich ist, wenn m und n prim zu einander sind.

Es bleibt also nur noch der Fall zu untersuchen, wo $4LN - M^2$ gleich einer **negativen** Zahl $-B$ ist. Ist dabei zunächst die Zahl B eine vollständiges Quadrat, so sind die Faktoren der Gröfse $Ly^2 + Myz + Nz^2$ rational, und die aufzulösende Gleichung besitzt die Form:

$$(my + nz)(fy + gz) = \pm H.$$

Nun ist ersichtlich, dafs sich die Auflösung dieser Gleichung auf die der beiden bestimmten Gleichungen:

$$my + nz = \vartheta$$
$$fy + gz = \pm \frac{H}{\vartheta}$$

reduciert, wo ϑ ein beliebiger Faktor von H ist. Man nehme also der Reihe nach für ϑ alle Teiler von H, die Einheit einbegriffen, und löse in Bezug auf jeden von ihnen die vorstehenden bestimmten Gleichungen auf. Hierdurch wird man mehrere Lösungen erhalten, wofern die sich ergebenden Werte von y und z ganze Zahlen sind. In keinem Falle aber kann die Anzahl dieser Lösungen die Anzahl der Teiler der Zahl H übersteigen.

79.

Nehmen wir nun an, dafs $M^2 - 4LN = 4A$ sei, wo A kein vollständiges Quadrat sein soll, so bietet die gegebene Gleichung

$$Ly^2 + Myz + Nz^2 = \pm H$$

zwei zu untersuchende Fälle dar, je nachdem $H < \sqrt{A}$ oder $> \sqrt{A}$ ist.

Es sei zuerst $H < \sqrt{A}$. In diesem Falle hat man nur eine Wurzel der Gleichung

$$Lx^2 + Mx + N = 0$$

in einen Kettenbruch zu entwickeln. Findet man unter den sich durch diese Rechnung ergebenden vollständigen Quotienten $\frac{\sqrt{A} + J}{D}$ einen mit dem Nenner $D = H$, so folgt daraus, daſs von den beiden Gleichungen:

$$Ly^2 + Myz + Nz^2 = + H$$
$$Ly^2 + Myz + Nz^2 = - H$$

wenigstens eine auflösbar ist, oder auch alle beide, wenn die erforderlichen Bedingungen erfüllt sind. Diese Bedingungen haben wir im § 9 angegeben, ebenso die Formeln, welche die vollständigen Werte von y und z enthalten, und wir haben bemerkt, daſs diese Formeln das Resultat der Entwicklung beider Wurzeln der Gleichung

$$Lx^2 + Mx + N = 0$$

in sich schlieſsen, so daſs man nur eine zu entwickeln braucht.

Die Zahl H kann innerhalb einer und derselben Periode mehrere Male unter den Werten von D vorkommen; alsdann ergeben sich daraus ebenso viele verschiedene Lösungen der gegebenen Gleichung. Kommt dieselbe aber unter diesen Werten gar nicht vor, so folgt daraus mit Sicherheit, daſs die gegebene Gleichung, weder wenn die rechte Seite $+ H$, noch wenn sie $- H$ ist, auflösbar ist.

Dieser erste Fall, in welchem $H < \sqrt{A}$, erledigt sich also unmittelbar und mit groſser Leichtigkeit allein durch die Kettenbruchentwicklung einer Wurzel der Gleichung $Lx^2 + Mx + N = 0$. Man kann sogar bemerken, daſs diese Lösung nur y und z als relative Primzahlen voraussetzt (denn da $\frac{y}{z}$ einem Näherungsbruche $\frac{p}{q}$ gleichgesetzt ist, so muſs es stets ein irreduktibler Bruch sein, da ja $pq^0 - p^0q = \pm 1$), und daſs sie somit nicht erfordert, daſs z und H prim zu einander seien. Hierdurch kann man sich also der Mühe überheben, die oben in No. 75 erwähnte, auf die gemeinsamen Faktoren von L und H sich beziehende Zerlegung auszuführen, und erhält durch eine einzige Rechnung die Lösung aller Gleichungen dieser Art. Es muſs jedoch, wie wir vorausgesetzt haben, $H < \sqrt{A}$ sein; ferner muſs man, wenn H einen quadratischen Faktor ϑ^2 besitzt, wie bereits angegeben, $y = \vartheta y'$, $z = \vartheta z'$, $H = \vartheta^2 H'$ setzen und auf demselben Wege eine jede Gleichung $Ly'^2 + My'z' + Nz'^2 = \pm H'$ für jeden quadratischen Faktor ϑ^2, welcher H teilen kann, auflösen.

80.

Ist zweitens $H > \sqrt{A}$, so setze man voraus, dafs die Gleichung, wie in No. 75 angegeben, vorbereitet ist, so dafs y und z ebenso wie z und H prim zu einander sind. Dann kann man

$$y = nz + Hu$$

setzen und sogar die Bedingung hinzufügen, dafs n nicht gröfser sein solle wie $\frac{1}{2}H$. Denn die vorstehende Gleichung würde bestehen, wenn man $n - \alpha H$ an Stelle von n und $u + \alpha z$ an Stelle von u setzte. Nun kann man aber offenbar α derart wählen, dafs $n - \alpha H$ zwischen $+\frac{1}{2}H$ und $-\frac{1}{2}H$ enthalten ist. Substituiert man also den Wert von y in die gegebene Gleichung und dividiert man das Resultat durch H, so erhält man:

$$\left(\frac{Ln^2 + Mn + N}{H}\right) z^2 + (2nL + M)\, zu + LHu^2 = \pm 1.$$

Da z und H prim zu einander sind, so kann diese Gleichung nur stattfinden, wenn

$$\frac{Ln^2 + Mn + N}{H}$$

eine ganze Zahl ist. Man gebe also n alle ganzzahligen Werte von $-\frac{1}{2}H$ bis $+\frac{1}{2}H$; giebt es unter diesen keinen, für welchen $Ln^2 + Mn + N$ durch H teilbar wird, so kann man mit Gewifsheit behaupten, dafs die gegebene Gleichung nicht auflösbar ist. Findet man dagegen einen oder mehrere Werte von n, welche diese Bedingung erfüllen, so mufs man nach einander diese verschiedenen Werte nehmen und für jeden eine besondere Rechnung anstellen, gleich als ob die gegebene Gleichung in ebenso viele verschiedene Gleichungen transformiert wäre.

Setzt man zur Abkürzung:

$$Ln^2 + Mn + N = fH,$$
$$2Ln + M = g$$
$$LH = h,$$

so wird die aufzulösende Gleichung für jeden Wert von n:

$$fz^2 + gzu + hu^2 = \pm 1,$$

wobei zu beachten ist, dafs man stets

$$g^2 - 4fh = M^2 - 4LN = 4A$$

hat.

Wir haben im § 9 eine Methode zur Auflösung dieser Gleichung, im Falle sie möglich ist, angegeben, und dieselben Bemerkungen, die wir für den Fall $D < \sqrt{A}$ gemacht haben, sind in gleicher Weise anwendbar für den Fall, wo $D = 1$ ist. Mithin haben wir hier nichts weiter hinzuzufügen, da man leicht erkennt, dafs man, nachdem die allgemeinen Werte von z und u gefunden sind, daraus unmittelbar die Werte der unbestimmten Zahlen in der gegebenen Gleichung erhält und zwar ebenfalls in ganzen Zahlen ausgedrückt.

81.

Beispiel.

Es sei die Aufgabe gestellt, die Gleichung:

$$2x^2 - 23y^2 = 105$$

in ganzen Zahlen aufzulösen.

Diese Gleichung gehört zum vorhergehenden Falle; sie läfst sich nicht in mehrere andere zerlegen, da 105 keinen quadratischen Teiler und ferner mit dem Koefficienten 2 keinen gemeinsamen Teiler hat. Man setze also:

$$x = ny - 105z,$$

und bestimme $n < \frac{105}{2}$ so, dafs $\frac{2n^2 - 23}{105}$ eine ganze Zahl wird. Später werden wir mehrere Hülfsmittel angeben, um derartige Untersuchungen zu erleichtern; für den Augenblick bemerken wir nur, dafs, da 105 das Produkt der Primzahlen 3, 5, 7 ist, man gesondert drei solche Werte von n suchen mufs, dafs

$$\frac{2n^2 - 23}{3}, \quad \frac{2n^2 - 23}{5}, \quad \frac{2n^2 - 23}{7}$$

ganze Zahlen werden. Diese Werte sind resp.

$$n = 3\alpha \pm 1, \quad n = 5\beta \pm 2, \quad n = 7\gamma \pm 1,$$

wo die Zahlen α, β, γ beliebig sind. Diese Formeln sind leicht mit einander zu vereinigen, und da es genügt, die Werte von n, welche positiv und $< \frac{105}{2}$ sind, zu betrachten, so giebt die letzte Formel:

$$n = 6,\ 8,\ 13,\ 15,\ 20,\ 22,\ 27,\ 29,\ 34,\ 36,\ 41,\ 43,\ 48,\ 50.$$

Hieraus sind alle Zahlen auszuscheiden, welche der zweiten Formel nicht genügen, oder welche durch 5 geteilt nicht den Rest ± 2 lassen. Mithin reducieren sich die vierzehn vorstehenden Werte auf die folgenden:

$$n = 8,\ 13,\ 22,\ 27,\ 43,\ 48.$$

Um endlich der ersten Formel zu genügen, sind alle durch 3 teilbaren Zahlen zu unterdrücken, so dafs nur die vier Werte übrig bleiben:

$$n = 8,\ 13,\ 22,\ 43.$$

Es sei also erstens $n = 8$ und $x = 8y - 105z$.

Alsdann ist die transformierte Gleichung:

$$y^2 - 32yz + 210z^2 = 1.$$

Jedesmal also, wenn man auf eine Gleichung von der Form

$$y^2 - 2fyz + gz^2 = 1$$

kommt, ist man sicher, dafs die Lösung stets möglich ist; denn setzt man:

$$y - fz = u,$$

so wird die Gleichung:

$$u^2 - Az^2 = 1,$$

und diese ist immer auflösbar. Im gegenwärtigen Falle findet man mit Hülfe der Formeln in No. 69:

$$y = \Phi \pm 16\Psi$$

$$z = \pm \Psi$$

$$(24335 + 3588\sqrt{46})^n = \Phi + \Psi\sqrt{46},$$

und hieraus ergiebt sich als erste Lösung der gegebenen Gleichung:

$$x = 8\Phi \pm 23\Psi$$

$$y = \Phi \pm 16\Psi.$$

Es sei zweitens $n = 13$ und $x = 13y - 105z$.

Dann ist die transformierte Gleichung:

$$3y^2 - 52yz + 210z^2 = 1.$$

Um dieselbe aufzulösen, mufs man eine Wurzel der Gleichung

$$3x^2 - 52x + 210 = 0$$

in einen Kettenbruch entwickeln. Das Verfahren hierzu, sowie die Berechnung der Näherungsbrüche, nur bis dahin, wo man $D = 1$ findet, ausgedehnt, stellt sich folgendermafsen dar:

$$x = \frac{\sqrt{46} + 26}{3} = 10 + \quad , \qquad 1 : 0$$

$$\frac{\sqrt{46} + 4}{10} = 1 + \quad , \qquad 10 : 1$$

$$\frac{\sqrt{46} + 6}{1} = 12 + \quad , \qquad 11 : 1$$

u. s. w. u. s. w.

Hiernach sind die Zahlen, welche in die Formeln der No. 69 einzusetzen sind, die folgenden:

$$p = 11, \quad q = 1, \quad a = 3, \quad b = -26, \quad c = 210, \quad A = 46.$$

Ferner hatten wir bereits beim ersten Falle gefunden, dafs die kleinsten der Gleichung

$$\varphi^2 - 46\psi^2 = \pm 1$$

genügenden Zahlen sind:

$$\varphi = 24335, \quad \psi = 3588,$$

und diese geben:

$$\varphi^2 - 46\psi^2 = +1.$$

Da man zugleich $pq^0 - p^0 q = +1$ hat, so ist die gegebene Gleichung $3y^2 - 52yz + 210z^2 = +1$ auflösbar (sie würde es nicht sein, wenn die rechte Seite -1 wäre). Setzt man also immer:

$$(24335 + 3588\sqrt{46})^n = \Phi + \Psi\sqrt{46},$$

so hat man, wenn man die Werte einsetzt:

$$y = 11\Phi \pm 76\Psi$$
$$z = \Phi \pm 7\Psi.$$

Hieraus ergiebt sich als zweite Lösung:

$$x = 38\Phi \pm 253\Psi$$
$$y = 11\Phi \pm 76\Psi.$$

Man beachte, dafs man die Werte von y und z unmittelbar aus der Rechnung für die Kettenbruchentwicklung hätte finden können. Denn wenn man an Stelle des vollständigen Quotienten $\frac{\sqrt{46}+6}{1}$, welcher dem Näherungsbruch $\frac{11}{1}$ entspricht, den angenäherten Wert $\frac{\Phi}{\Psi} + 6$ setzt, und wenn man darauf mit Hülfe dieses als vollständig betrachteten Quotienten den auf $\frac{11}{1}$ folgenden Näherungsbruch berechnet, so findet man diesen Bruch gleich

$$\frac{11\left(6 + \frac{\Phi}{\Psi}\right) + 10}{1\left(6 + \frac{\Phi}{\Psi}\right) + 1},$$

und dieser reduciert sich auf:

$$\frac{11\Phi + 76\Psi}{\Phi + 7\Psi}.$$

Dies ist der allgemeine Wert von $\frac{y}{z}$; man hat darin nur noch Ψ das doppelte Zeichen $\pm$ zu geben. Es würde leicht sein zu be-

weisen, dafs dieses Verfahren, welches uns der Mühe überhebt, auf die allgemeinen Formeln zurückzugehen, vollständig mit den letzteren übereinstimmt und somit an deren Stelle gesetzt werden kann, selbst für einen beliebigen Wert von D.

Ist drittens $n = 22$ und $x = 22y - 105z$, so wird die transformierte Gleichung:

$$9y^2 - 88yz + 210z^2 = 1.$$

Man entwickele demnach eine Wurzel der Gleichung

$$9x^2 - 88x + 210 = 0$$

in einen Kettenbruch, bis man einen vollständigen Quotienten mit dem Nenner 1 findet, und berechne darnach die Näherungsbrüche wie folgt:

$$x = \frac{\sqrt{46} + 44}{9} = 5 + \quad , \quad 1 : 0$$

$$\frac{\sqrt{46} + 1}{5} = 1 + \quad , \quad 5 : 1$$

$$\frac{\sqrt{46} + 4}{6} = 1 + \quad , \quad 6 : 1$$

$$\frac{\sqrt{46} + 2}{7} = 1 + \quad , \quad 11 : 2$$

$$\frac{\sqrt{46} + 5}{3} = 3 + \quad , \quad 17 : 3$$

$$\frac{\sqrt{46} + 4}{10} = 1 + \quad , \quad 62 : 11$$

$$\frac{\sqrt{46} + 6}{1} = 12 + \quad , \quad 79 : 14.$$

Dieser letztere Näherungsbruch $\frac{79}{14}$ genügt der gegebenen Gleichung, da er von ungerader Ordnung und somit $pq^0 - p^0q = +1$ ist. Gemäfs der beim vorhergehenden Falle gemachten Bemerkung nehme man jetzt an, dafs der dem letzten Näherungsbruche $\frac{79}{14}$ entsprechende Quotient $\frac{\Phi}{\Psi} + 6$ sei. Dann ergiebt sich daraus der darauf folgende Bruch:

$$\frac{y}{z} = \frac{79\left(6 + \frac{\Phi}{\Psi}\right) + 62}{14\left(6 + \frac{\Phi}{\Psi}\right) + 11} = \frac{79\Phi + 536\Psi}{14\Phi + 95\Psi},$$

und hieraus folgt allgemein:

$$y = 79\Phi \pm 536\Psi, \quad z = 14\Phi \pm 95\Psi,$$

und es ist somit die dritte Lösung:

$$x = 268\Phi \pm 1817\Psi$$
$$y = 79\Phi \pm 536\Psi.$$

Ist viertens $n = 43$ und $x = 43y - 105z$, so ist die transformierte Gleichung:

$$35y^2 - 172yz + 210z^2 = 1.$$

Man hat also eine Wurzel der Gleichung

$$35x^2 - 172x + 210 = 0$$

zu entwickeln, bis man einen vollständigen Quotienten $\frac{\sqrt{46} + J}{D}$ findet, in welchem D gleich 1 ist. Die Rechnung stellt sich folgendermaſsen:

$$x = \frac{\sqrt{46} + 86}{35} = 2 + \quad, \qquad 1 : 0$$
$$\frac{\sqrt{46} - 16}{-6} = 1 + \quad, \qquad 2 : 1$$
$$\frac{\sqrt{46} + 10}{9} = 1 + \quad, \qquad 3 : 1$$
$$\frac{\sqrt{46} - 1}{5} = 1 + \quad, \qquad 5 : 2$$
$$\frac{\sqrt{46} + 6}{2} = 6 + \quad, \qquad 8 : 3$$
$$\frac{\sqrt{46} + 6}{5} = 2 + \quad, \qquad 53 : 20$$
$$\frac{\sqrt{46} + 4}{6} = 1 + \quad, \qquad 114 : 43$$
$$\frac{\sqrt{46} + 2}{7} = 1 + \quad, \qquad 167 : 63$$
$$\frac{\sqrt{46} + 5}{3} = 3 + \quad, \qquad 281 : 106$$
$$\frac{\sqrt{46} + 4}{10} = 1 + \quad, \qquad 1010 : 381$$
$$\frac{\sqrt{46} + 6}{1} = 12 + \quad, \qquad 1291 : 487.$$

Dieser elfte Näherungsbruch genügt der gegebenen Gleichung:

$$35y^2 - 172yz + 210z^2 = +1,$$

da er von ungerader Ordnung ist. Man erhält sodann die vollständige Lösung, wenn man $6 + \frac{\Phi}{\Psi}$ an die Stelle des entsprechenden Quotienten setzt. Dies giebt:

$$\frac{y}{z} = \frac{1291\left(6+\frac{\Phi}{\Psi}\right)+1010}{487\left(6+\frac{\Phi}{\Psi}\right)+381} = \frac{1291\Phi+8756\Psi}{487\Phi+3303\Psi},$$

und hieraus folgt die vierte Lösung:

$$x = 4378\Phi \pm 29693\Psi$$
$$y = 1291\Phi \pm 8756\Psi.$$

Es dürfte die Bemerkung angebracht sein, dafs man schneller und einfacher zu dieser vierten Lösung gelangt sein würde, wenn man die andere Wurzel derselben Gleichung entwickelt hätte. Die Rechnung stellt sich so:

$$x = \frac{\sqrt{46}-86}{-35} = 2+\quad, \quad 1:0$$
$$\frac{\sqrt{46}+16}{6} = 3+\quad, \quad 2:1$$
$$\frac{\sqrt{46}+2}{7} = 1+\quad, \quad 7:3$$
$$\frac{\sqrt{46}+5}{3} = 3+\quad, \quad 9:4$$
$$\frac{\sqrt{46}+4}{10} = 1+\quad, \quad 34:15$$
$$\frac{\sqrt{46}+6}{1} = 12+\quad, \quad 43:19.$$

Hieraus folgt:

$$\frac{y}{z} = \frac{43\left(6+\frac{\Phi}{\Psi}\right)+34}{19\left(6+\frac{\Phi}{\Psi}\right)+15} = \frac{43\Phi+292\Psi}{19\Phi+129\Psi},$$

und man erhält als vierte Lösung:

$$x = 146\Phi \pm 989\Psi$$
$$y = 43\Phi \pm 292\Psi.$$

Diese Formeln, welche auf dasselbe hinauskommen wie die obigen, sind einfacher als die, welche wir mittelst der andern Wurzel gefunden haben. Die Übereinstimmung beider kann man übrigens beweisen, indem man annimmt, dafs die Φ und Ψ dieser Formel einem Werte von n entsprechen, der um eine Einheit kleiner ist als das n in den Werten von Φ und Ψ in der andern Formel. Unterscheidet man daher diese durch Φ' und Ψ', so kann man setzen:

$$\Phi + \Psi\sqrt{46} = (\Phi' + \Psi'\sqrt{46})\,(24335 - 3588\sqrt{46}).$$

Stellt man diese verschiedenen Resultate zusammen, so erhält man sämtliche Lösungen der gegebenen Gleichung:

$$2x^2 - 23y^2 = 105.$$

Dieselben sind in den folgenden Formeln, in denen

$$(24335 + 3588\sqrt{46})^n = \Phi + \Psi\sqrt{46}$$

gesetzt ist, enthalten:

$$\begin{aligned} x &= 8\Phi \pm 23\Psi \quad, & y &= \Phi \pm 16\Psi \\ x &= 38\Phi \pm 253\Psi \quad, & y &= 11\Phi \pm 76\Psi \\ x &= 268\Phi \pm 1817\Psi \quad, & y &= 79\Phi \pm 536\Psi \\ x &= 146\Phi \pm 989\Psi \quad, & y &= 43\Phi \pm 292\Psi. \end{aligned}$$

Dieselbe Gleichung oder eine äquivalente Gleichung ($p^2 - 46q^2 = 210$) ist in den Abhandlungen der Berliner Akademie vom Jahre 1767 gelöst. Das daselbst pag. 263 gegebene Resultat stellt acht Lösungen dar.

Diese acht Lösungen reducieren sich auf die vier vorstehenden; überhaupt kann die Rechnung stets um die Hälfte abgekürzt werden, wenn man, wie wir es gethan haben, beachtet, dafs es überflüssig ist, beide Wurzeln derselben Gleichung in einen Kettenbruch zu entwickeln, und dafs die Entwicklung einer einzigen ausreicht, um das aus beiden sich ergebende Resultat zu erhalten.

82.

Als ferneres Beispiel wollen wir noch die Gleichung nehmen:

$$67y^2 - 227yz + 191z^2 = 5.$$

Durch Vergleichung derselben mit der allgemeinen Formel (No. 67) ergiebt sich:

$$f = 67, \quad g = -227, \quad h = 191, \quad D = 5.$$

$$A = \frac{g^2}{4} - fh = \frac{341}{4}, \quad D < \sqrt{A}.$$

Man kann demnach diese Gleichung durch Entwicklung einer Wurzel der Gleichung

$$67x^2 - 227x + 191 = 0$$

in einen Kettenbruch auflösen. Die Rechnung, bis zu dem Punkte, wo man die sich bis ins Unendliche wiederholende Periode gefunden hat, fortgesetzt, stellt sich folgendermafsen:

$$
\begin{array}{rll}
x = \dfrac{113\frac{1}{2} + \frac{1}{2}\sqrt{341}}{67} = & 1 + \,, & 1 : \;\; 0 \\[2ex]
\dfrac{-46\frac{1}{2} + \frac{1}{2}\sqrt{341}}{-31} = & 1 + \,, & 1 : \;\; 1 \\[2ex]
\dfrac{15\frac{1}{2} + \frac{1}{2}\sqrt{341}}{5} = & 4 + \,, & 2 : \;\; 1 \\[2ex]
\dfrac{4\frac{1}{2} + \frac{1}{2}\sqrt{341}}{13} = & 1 + \,, & 9 : \;\; 5 \\[2ex]
\dfrac{8\frac{1}{2} + \frac{1}{2}\sqrt{341}}{1} = & 17 + \,, & 11 : \;\; 6 \\[2ex]
\dfrac{8\frac{1}{2} + \frac{1}{2}\sqrt{341}}{13} = & 1 + \,, & 196 : 107 \\[2ex]
\dfrac{4\frac{1}{2} + \frac{1}{2}\sqrt{341}}{5} = & 2 + \,, & 207 : 113 \\[2ex]
\dfrac{5\frac{1}{2} + \frac{1}{2}\sqrt{341}}{11} = & 1 + \,, & 610 : 333 \\[2ex]
\dfrac{5\frac{1}{2} + \frac{1}{2}\sqrt{341}}{5} = & 2 + \,, & 817 : 446 \\[2ex]
\dfrac{4\frac{1}{2} + \frac{1}{2}\sqrt{341}}{13} = & 1 + \,, & \text{u. s. w.}
\end{array}
$$

Da der vollständige Quotient $\frac{4\frac{1}{2} + \frac{1}{2}\sqrt{341}}{13}$ zu den bereits gefundenen gehört, so ist die Rechnung beendet, und man sieht, dafs man unmittelbar nach den ersten Gliedern 1, 1, 4 die sich bis ins Unendliche immer wiederholende Periode 1, 17, 1, 2, 1, 2 erhält.

Sucht man jetzt die Zahl 5 unter den Nennern der vollständigen Quotienten, so sieht man, dafs der dritte, der siebente und der neunte Näherungsbruch der gegebenen Gleichung genügen können. Der siebente und neunte, welche derselben Periode angehören, genügen in der That, da sie von ungerader Ordnung sind, und da in dem Werte von x die Wurzelgröfse positiv genommen worden ist. Was den dritten anbetrifft, so genügt er zwar ebenfalls; wir sehen jedoch von ihm ab, da es ausreicht, die durch die Glieder einer und derselben Periode gegebenen Lösungen zu betrachten, und alle andern in diesen enthalten sein müssen. Man sehe hierüber den folgenden Paragraphen.

Man erhält somit mittelst des siebenten Näherungsbruches:

$$p = 207, \quad q = 113,$$

und berechnet man wie gewöhnlich den Wert der von diesem Gliede ab gerechneten Periode:

Periode: 2, 1, 2, 1, 17, 1

Näherungsbrüche: $\frac{1}{0}, \frac{2}{1}, \frac{3}{1}, \frac{8}{3}, \frac{11}{4}, \frac{195}{71}, \frac{206}{75}$,

so findet man:

$$\frac{\alpha}{\beta} = \frac{206}{75}, \quad \beta^0 = 71, \quad \varphi = \frac{\alpha + \beta^0}{2} = 138\frac{1}{2}, \quad \psi = \frac{\beta}{D} = 15.$$

Man erhält daher:

$$\left(\frac{277}{2} + \frac{15}{2}\sqrt{341}\right)^n = \Phi + \frac{1}{2}\Psi\sqrt{341}.$$

Man hat zu gleicher Zeit:

$$\varphi^2 - A\psi^2 = +1,$$

und dies beweist, dafs die gegebene Gleichung auflösbar ist, wenn die rechte Seite $+5$ ist, dafs sie es aber nicht sein würde, wenn ihre rechte Seite -5 lautete. Setzt man, nachdem dieses festgestellt ist, die gefundenen Werte in die Formel der No. 67 ein, so erhält man als erste Lösung der gegebenen Gleichung:

$$y = 207\Phi \pm 3823 \cdot \frac{1}{2}\Psi$$

$$z = 113\Phi \pm 2087 \cdot \frac{1}{2}\Psi.$$

Verfährt man in derselben Weise mit dem neunten Näherungsbruche $\frac{817}{446}$, so ergiebt sich die zweite Lösung:

$$y = 817\Phi \pm 15087 \cdot \frac{1}{2}\Psi$$

$$z = 446\Phi \pm 8236 \cdot \frac{1}{2}\Psi.$$

Diese letzteren Formeln enthalten die Lösung $\frac{2}{1}$, die wir in dem unregelmäfsigen Teile des Kettenbruches bemerkt haben. Setzt man nämlich $n = 1$, $\Phi = \frac{277}{2}$, $\pm\Psi = -15$, so findet man $y = 2$, $z = 1$. Daraus läfst sich vermuten, dafs die zweite allgemeine Lösung auf eine einfachere Form gebracht werden kann. Hierüber verschafft man sich leicht Gewifsheit, wenn man an Stelle von Φ und Ψ die analogen Gröfsen, welche einem um eine Einheit verschiedenen Werte von n entsprechen, nimmt. Es ergiebt sich:

$$y = 2\Phi \pm 72 \cdot \frac{1}{2}\Psi$$

$$z = \Phi \pm 41 \cdot \frac{1}{2}\Psi.$$

83.

Aus dem, was in diesem Paragraphen bewiesen worden ist, erkennt man, dafs, wenn die betreffenden Gleichungen möglich sind, ihre Auflösung durch ein oder mehrere Formelsysteme von der Form

$$y = a'\,\Phi + b'\,\Psi$$
$$z = a''\Phi + b''\Psi$$

gegeben wird. Dabei sind die Zahlen a', b', a'', b'' konstant und die Gröfsen Φ und Ψ bestimmen sich durch die Gleichung:

$$(\varphi + \psi\sqrt{A})^n = \Phi + \Psi\sqrt{A},$$

in welcher n eine unbestimmte Zahl, und wo jederzeit $\varphi^2 - A\psi^2 = \pm 1$ und demnach auch $\Phi^2 - A\Psi^2 = (\pm 1)^n = +1$ oder -1 ist.

In den allgemeinen Formeln kann man Ψ nach Belieben negativ oder positiv nehmen und somit Ψ mit dem doppelten Vorzeichen ± 1 versehen. Dies kommt auf dasselbe hinaus, als wenn man das Vorzeichen von Ψ als bestimmt ansieht und für n irgendwelche positive oder negative Werte nimmt. Denn es ist:

$$(\varphi + \psi\sqrt{A})^{-n} = (\varphi^2 - A\psi^2)^{-n}\,(\varphi - \psi\sqrt{A})^n = (\pm 1)^n\,(\Phi - \Psi\sqrt{A}),$$

und mithin ist die Änderung des Vorzeichens von n gleichbedeutend mit der Änderung des Vorzeichens von Ψ, da es auf das Zeichen von $(\pm 1)^n$, mit welchem das Ganze behaftet ist, nicht ankommt; denn wie aus der Natur der gegebenen Gleichung sich ergiebt, kann man immer das Zeichen von y und das von z gleichzeitig ändern.

Es folgt hieraus, dafs die verschiedenen, in einem solchen Formelsystem, wie das vorhergehende, enthaltenen Werte von y und z zwei Reihen bilden, die sich ins Unendliche in positiver wie in negativer Richtung erstrecken, und von denen jedes Glied einem bestimmten, positiven oder negativen Werte von n entspricht, in folgender Weise:

n	$\cdots$	$-3,$	$-2,$	$-1,$	$0,$	$1,$	$2,$	$3,$	$\cdots$
y	$\cdots$	$'''p,$	$''p,$	$'p,$	$p,$	$p_1,$	$p_2,$	$p_3,$	$\cdots$
z	$\cdots$	$'''q,$	$''q,$	$'q,$	$q,$	$q_1,$	$q_2,$	$q_3,$	$\cdots$

Übrigens beruht die einfachste Art, die Zahlenwerte dieser Glieder zu berechnen, auf der Anwendung des No. 62 gefundenen Gesetzes, welches $p_2 = 2\varphi p_1 \mp p$ (wo das Zeichen $\mp$ dem von $\varphi^2 - A\psi^2$ entgegengesetzt ist) giebt. Diese Formel, in welcher p, p_1, p_2 allgemein drei aufeinanderfolgende Glieder bezeichnen, kann zur Fortsetzung einer dieser Reihen sei es nach rechts oder nach links hin dienen. Dasselbe Gesetz findet bei der andern Reihe statt.

§ 12.

Beweis eines in den vorhergehenden Paragraphen vorausgesetzten Satzes.

84.

Wir haben bisher angenommen, dafs, wenn es möglich ist, der Gleichung

$$fy^2 + gyz + hz^2 = \pm H,$$

in welcher y und z als relative Primzahlen und $H < \frac{1}{2}\sqrt{g^2 - 4fh}$ vorausgesetzt ist, Genüge zu leisten, der Bruch $\frac{y}{z}$ stets unter den Näherungsbrüchen einer Wurzel der Gleichung

$$fx^2 + gx + h = 0$$

enthalten ist. Dieser Satz besitzt grofse Ähnlichkeit mit dem in No. 10. Indessen ist es durchaus notwendig zu beweisen, dafs er allgemein richtig ist, abgesehen von einer geringfügigen Ausnahme, die wir erwähnen werden.

Es möge f eine positive Zahl, g und h nach Belieben positive oder negative Zahlen bedeuten; ferner sei $\frac{p}{q}$ ein gegebener Bruch, dessen Zähler und Nenner prim zu einander sind und der Gleichung

$$fp^2 + gpq + hq^2 = \pm H$$

genügen. Wir nehmen an, dafs man $\frac{p}{q}$ in einen Kettenbruch entwickle, und dafs die bei dieser Rechnung sich ergebenden Quotienten $\alpha, \beta, \ldots \lambda, \mu$ seien. Mittelst dieser Quotienten berechne man in der gewöhnlichen Weise die Näherungsbrüche von $\frac{p}{q}$. Bezeichnet man mit $\frac{p^0}{q^0}$ denjenigen Näherungsbruch, welcher $\frac{p}{q}$ unmittelbar vorangeht, so kann man, wie wir bereits (No. 9) gesehen haben, nach Belieben $pq^0 - p^0q = +1$ oder $pq^0 - p^0q = -1$ setzen.

Dies vorausgeschickt, betrachten wir dieselben aufeinanderfolgenden Brüche $\frac{p^0}{q^0}, \frac{p}{q}$ als zur Entwicklung von x in einen Kettenbruch gehörig. Ist z der vollständige Quotient, welcher dem letzteren Bruche entspricht, so mufs demnach sein:

$$x = \frac{pz + p^0}{qz + q^0} \text{ oder } z = \frac{q^0x - p^0}{p - qx}.$$

Nun wird die Annahme, dafs $\frac{p^0}{q^0}, \frac{p}{q}$ zwei aufeinanderfolgende Näherungsbrüche von x seien, berechtigt sein, wenn der soeben gefundene

Wert von z positiv und gröſser als die Einheit ist. Denn dies ist die Bedingung, welcher alle aus der Kettenbruchentwicklung einer beliebigen Gröſse hervorgehenden vollständigen Quotienten unterworfen sein müssen. Es handelt sich daher darum zu untersuchen, ob diese Bedingung erfüllt ist.

Aus der vorstehenden Gleichung erhält man:

$$z + \frac{q^0}{q} = \frac{pq^0 - p^0 q}{q^2\left(\frac{p}{q} - x\right)}.$$

Setzt man nun stets:

$$A = \frac{1}{4}g^2 - fh,$$

so ist:

$$x = \frac{-\frac{1}{2}g \pm \sqrt{A}}{f}.$$

Substituiert man diesen Wert für x und schafft alsdann das Wurzelzeichen aus dem Nenner fort, so wird:

$$z + \frac{q^0}{q} = \frac{pq^0 - p^0 q}{2} \cdot \frac{2f\frac{p}{q} + g \pm 2\sqrt{A}}{fp^2 + gpq + hq^2}.$$

In dieser Gleichung kann man das Zeichen von $\sqrt{A}$ nach Belieben wählen, da es freisteht, für x die eine oder die andere Wurzel der Gleichung $fx^2 + gx + h = 0$ zu nehmen, und der Wert von z in beiden Fällen verschieden ist. Da ferner

$$fp^2 + gpq + hq^2 = \pm H$$

ist, so giebt diese Gleichung:

$$\frac{2fp}{q} + g = \pm 2\sqrt{A \pm \frac{fH}{q^2}}.$$

Folglich erhält man:

$$z + \frac{q^0}{q} = (pq^0 - p^0 q) \cdot \frac{\pm\sqrt{A} \pm \sqrt{A \pm \frac{fH}{q^2}}}{\pm H}.$$

Von diesen verschiedenen unbestimmt gelassenen Zeichen ist nur dasjenige von $\pm\sqrt{A}$ willkürlich, da das Zeichen von H von der gegebenen Gleichung abhängt und das von $\sqrt{A \pm \frac{fH}{q^2}}$ in gleicher Weise durch den Wert von $\frac{2fp}{q} + g$ bedingt ist. Da es aber von Wichtigkeit ist, den gröſsten Wert von z zu betrachten, so nehme man das Zeichen von $\sqrt{A}$ gleich dem von $\sqrt{A \pm \frac{fH}{q^2}}$. Alsdann ist

die rechte Seite unserer Gleichung notwendigerweise von der Form:

$$\pm (pq^0 - p^0 q) \frac{\sqrt{A} + \sqrt{A \pm \frac{fH}{q^2}}}{H}.$$

Endlich kann man diese Gröfse stets positiv annehmen, da man nach Belieben $pq^0 - p^0 q = +1$ oder -1 setzen kann. Man erhält daher in allen Fällen:

$$z + \frac{q^0}{q} = \frac{\sqrt{A} + \sqrt{A \pm \frac{fH}{q^2}}}{H}.$$

85.

Ist erstens $fp^2 + gpq + hq^2 = +H$, so hat man:

$$z + \frac{q^0}{q} = \frac{\sqrt{A} + \sqrt{A + \frac{fH}{q^2}}}{H}.$$

Die rechte Seite ist gröfser als $\frac{2\sqrt{A}}{H}$ und folglich > 2, da $H < \sqrt{A}$ ist; ferner ist $q^0 < q$. Mithin ist der Wert von z positiv und gröfser als 1. Demnach ist der gegebene Bruch $\frac{p}{q}$, welcher der Gleichung $fp^2 + gpq + hq^2 = +H$ genügt, stets einer der Näherungsbrüche von einer Wurzel der Gleichung $fx^2 + gx + h = 0$. Dieser Schlufs erleidet keine Ausnahme, so lange die rechte Seite H positiv ist.

86.

Ist zweitens $fp^2 + gpq + hq^2 = -H$, so hat man:

$$z + \frac{q^0}{q} = \frac{\sqrt{A} + \sqrt{A - \frac{fH}{q^2}}}{H}.$$

Nun sieht man, dafs, wenn der Wert von q^2 hinreichend grofs wird im Verhältnis zu $\frac{fH}{A}$ (kleiner kann er niemals sein), der Wert von $z + \frac{q^0}{q}$ sehr nahe gleich $\frac{2\sqrt{A}}{H}$ ist, so dafs man erhält:

$$z = \frac{2\sqrt{A}}{H} - \frac{q^0}{q},$$

eine Gröfse, welche positiv und gröfser als die Einheit ist.

Übrigens ist es, ohne das Glied $\frac{fH}{q^2}$ zu vernachlässigen, leicht,

die Grenze von q anzugeben, für welche z noch positiv und gröfser als 1 ist. Dazu bringen wir z auf die Form:

$$z = \frac{2\sqrt{A}}{H} - \frac{1+q^0}{q} + \frac{1}{q} - \frac{\sqrt{A}}{H} + \frac{1}{H}\sqrt{A - \frac{fH}{q^2}}.$$

Da

$$\sqrt{A} > H \text{ und } \frac{1+q^0}{q} < 1 \text{ oder höchstens } = 1$$

ist, so ist offenbar z positiv und gröfser als 1, wenn die Gröfse $\sqrt{A - \frac{fH}{q^2}}$ gröfser als $\sqrt{A} - \frac{H}{q}$ ist. Ist also:

$$\sqrt{A - \frac{fH}{q^2}} > \sqrt{A} - \frac{H}{q},$$

so folgt hieraus, wenn man ins Quadrat erhebt und vereinfacht:

$$q > \frac{f+H}{2\sqrt{A}}.$$

So lange also q oberhalb dieser Grenze liegt, ist sicher immer der Wert von z positiv und gröfser als 1; ist dagegen $q < \frac{f+H}{2\sqrt{A}}$, so kann man im allgemeinen nicht mehr behaupten, dafs z gröfser als die Einheit ist.

87.

Wie beschaffen auch q sein möge, der Ausnahmefall wird **niemals** stattfinden, sobald f, wie wir voraussetzen, eine **positive** Zahl, h dagegen eine **negative** Zahl ist. Denn alsdann hat die gegebene Gleichung die Form:

$$fp^2 + gpq - h'q^2 = -H,$$

und diese ist dieselbe wie:

$$h'q^2 - gpq - fp^2 = +H.$$

Da somit diese Gleichung auf den ersten Fall zurückgeführt ist, so folgt daraus, dafs $\frac{q}{p}$ ein Näherungsbruch einer Wurzel der Gleichung

$$h'x^2 - gx - f = 0$$

ist. Mithin wird (indem man $\frac{1}{x}$ für x setzt) $\frac{p}{q}$ ein Näherungsbruch einer Wurzel der Gleichung

$$fx^2 + gx - h' = 0$$

sein.

88.

Wenn eine Gleichung

$$fy^2 + gyz + hz^2 = -H,$$

in welcher f und h positiv sind, aufgelöst werden soll, so kann man diese Gleichung immer (No. 58) in eine andere

$$ay'^2 + by'z' - cz'^2 = -H$$

transformieren, in welcher a und c positiv und überdies

$$b^2 + 4ac = g^2 - 4fh = 4A$$

ist. Diese Gleichung wird daher zu dem Falle der vorhergehenden Nummer gehören, und wenn überdies $H < \sqrt{A}$ ist, so werden alle Lösungen durch die Näherungsbrüche einer Wurzel der Gleichung

$$ax^2 + bx - c = 0$$

gegeben sein.

Man sieht hieraus, dafs der erwähnte Ausnahmefall, der übrigens nur sehr selten und für sehr kleine Werte von p und q eintritt, vollständig vermöge der bereits angegebenen Transformationen umgangen werden kann. Die Behauptung, dafs, wenn

$$H < \frac{1}{2}\sqrt{g^2 - 4fh}$$

ist, alle Lösungen der Gleichung

$$fy^2 + gyz + hz^2 = \pm H$$

durch die Näherungsbrüche einer Wurzel der Gleichung

$$fx^2 + gx + h = 0$$

gegeben werden, ist daher allgemein richtig.

89.

Es dürfte übrigens nicht überflüssig sein, ein dem erwähnten Ausnahmefalle unterliegendes Beispiel beizubringen, das uns zugleich Anlafs zu neuen Bemerkungen liefern wird. Es sei zu dem Zwecke die Gleichung gegeben:

$$1801y^2 - 3991yz + 2211z^2 = -3,$$

wobei

$$A = \frac{1}{4}g^2 - fh = \frac{37}{4}, \quad H = 3,$$

und somit $H < \sqrt{A}$ ist. Dieser Gleichung genügt man, indem man $y = 31$ und $z = 28$ setzt; indessen ist der Bruch $\frac{31}{28}$ nicht unter den Näherungsbrüchen einer Wurzel der Gleichung

$$1801x^2 - 3991x + 2211 = 0$$

enthalten. Denn die Entwicklung der größeren Wurzel giebt:

$$\begin{array}{rlr} x = \dfrac{1995\frac{1}{2} + \frac{1}{2}\sqrt{37}}{1801} = 1 + & , & 1:\ 0 \\ \dfrac{-194\frac{1}{2} + \frac{1}{2}\sqrt{37}}{-21} = 9 + & , & 1:\ 1 \\ \dfrac{5\frac{1}{2} + \frac{1}{2}\sqrt{37}}{1} = 8 + & , & 10:\ 9 \\ \dfrac{2\frac{1}{2} + \frac{1}{2}\sqrt{37}}{3} = 1 + & , & 81:73 \\ \text{u. s. w.} & & \text{u. s. w.,} \end{array}$$

und die der kleineren Wurzel giebt:

$$\begin{array}{rlr} x = \dfrac{-1995\frac{1}{2} + \frac{1}{2}\sqrt{37}}{-1801} = 1 + & , & 1:\ 0 \\ \dfrac{194\frac{1}{2} + \frac{1}{2}\sqrt{37}}{21} = 9 + & , & 1:\ 1 \\ \dfrac{-5\frac{1}{2} + \frac{1}{2}\sqrt{37}}{-1} = 2 + & , & 10:\ 9 \\ \dfrac{3\frac{1}{2} + \frac{1}{2}\sqrt{37}}{3} = 2 + & , & 21:19 \\ \dfrac{2\frac{1}{2} + \frac{1}{2}\sqrt{37}}{1} = 5 + & , & 52:47 \\ \text{u. s. w.} & & \text{u. s. w.} \end{array}$$

Man findet also weder bei der einen noch bei der andern Entwicklung den Näherungsbruch $\frac{31}{28}$, und dies steht im Einklang mit der Formel des Artikel 86, da hier 28, welches der Wert von q ist, kleiner ist als $\dfrac{f + H}{2\sqrt{A}} = \dfrac{1804}{\sqrt{37}}$.

Um diesen Übelstand zu vermeiden und zu bewirken, daſs die Lösung durch die Näherungsbrüche gegeben werde, genügt es, die Gröſse

$$1801y^2 - 3991yz + 2211z^2,$$

wenn nicht auf den einfachsten Ausdruck, so doch wenigstens auf eine Form zu bringen, in welcher die äuſseren Glieder von entgegengesetztem Vorzeichen sind. Dies erreicht man unmittelbar, indem man setzt:

$$\begin{aligned} y &= 10y' - 51z' \\ z &= \ \ 9y' - 46z'; \end{aligned}$$

denn alsdann reduciert sich die gegebene Gleichung auf die sehr einfache Form:

$$y'^2 + y'z' - 9z'^2 = -3.$$

Entwickelt man also eine Wurzel der Gleichung

$$x^2 + x - 9 = 0$$

in einen Kettenbruch, so erhält man:

$$\begin{array}{rll} x = \dfrac{-\frac{1}{2} + \frac{1}{2}\sqrt{37}}{1} = 2 + & , & 1:\ 0 \\[2ex] \dfrac{2\frac{1}{2} + \frac{1}{2}\sqrt{37}}{3} = 1 + & , & 2:\ 1 \\[2ex] \dfrac{\frac{1}{2} + \frac{1}{2}\sqrt{37}}{3} = 1 + & , & 3:\ 1 \\[2ex] \dfrac{2\frac{1}{2} + \frac{1}{2}\sqrt{37}}{1} = 5 + & , & 5:\ 2 \\[2ex] \dfrac{2\frac{1}{2} + \frac{1}{2}\sqrt{37}}{3} = 1 + & , & 28:11 \\[1ex] \text{u. s. w.} & & \text{u. s. w.} \end{array}$$

Beim Anblick der vollständigen Quotienten erkennt man, dafs der Näherungsbruch $\frac{2}{1}$ für $\frac{y'}{z'}$ genommen werden kann. Denn setzt man $y' = 2$, $z' = 1$, so hat man $y'^2 + y'z' - 9z'^2 = -3$ und hieraus folgt:

$$y = -31, \quad z = -28,$$

und dies ist die Lösung, welche mit Hülfe der Näherungsbrüche gefunden werden sollte.

Im Übrigen ist die allgemeine Lösung der Gleichung in y' und z', die aus der soeben ausgeführten Entwicklung abgeleitet werden kann, in den folgenden Formeln enthalten.

1) Setzt man:

$$(6 + \sqrt{37})^{2k} = F + G\sqrt{37},$$

so erhält man:

$$\begin{aligned} y' &= 2F \pm 16G \\ z' &= F \pm 5G, \end{aligned}$$

und hieraus folgt:

$$\begin{aligned} y &= -31F \mp 95G \\ z &= -28F \mp 86G. \end{aligned}$$

2) Setzt man:

$$(6 + \sqrt{37})^{2k+1} = F' + G'\sqrt{37},$$

so erhält man:

$$\begin{aligned} y' &= 3F' \pm 15G' \\ z' &= F' \pm 7G', \end{aligned}$$

und hieraus ergiebt sich:

$$y = -21F' \mp 207G'$$
$$z = -19F' \mp 187G'.$$

90.

Betrachtet man jetzt den soeben von uns bei diesem Beispiele verfolgten Weg genauer, so sieht man, dafs nach Vereinfachung der Form der aufzulösenden Gleichung die einfachsten Lösungen sich als die ersten unter den Näherungsbrüchen darbieten mufsten. Aus diesen ersten Lösungen hat sich mit Hülfe der gewöhnlichen Formeln die allgemeine Lösung ergeben, welche nichts anderes ist als der Ausdruck der verschiedenen der Aufgabe genügenden Näherungsbrüche, wenn diese Brüche der Reihe nach an derselben Stelle innerhalb sämtlicher Perioden genommen werden. Nun ist der so gefundene allgemeine Ausdruck, auf welche Weise man auch zu ihm gelangt sei, der einzige; er würde im Grunde derselbe sein, wenn man, um ihn zu finden, von besonderen Werten von p und q aus einer andern Periode als der ersten ausgegangen wäre. Um uns besser verständlich zu machen, nehmen wir die Gleichung:

$$y^2 - 3z^2 = 1,$$

der man durch folgende Werte der Reihe nach genügen kann:

$$\frac{y}{z} = \frac{2}{1}, \quad \frac{7}{4}, \quad \frac{26}{15}, \quad \frac{97}{56}, \quad \frac{362}{209}, \ldots$$

Geht man von der ersten Lösung $\frac{2}{1}$ aus, so würde der allgemeine Ausdruck dieser Werte

$$y = F, \quad z = G$$

sein, wo F und G durch die Gleichung

$$(2 + \sqrt{3})^n = F + G\sqrt{3}$$

bestimmt werden. In gleicher Weise kann man aber von dem besonderen Werte $\frac{26}{15}$ ausgehen und würde dann den allgemeinen Ausdruck aus der Gleichung

$$y + z\sqrt{3} = (26 + 15\sqrt{3})\,(F \pm G\sqrt{3})$$

erhalten, welche giebt:

$$y = 26F \pm 45G$$
$$z = 15F \pm 26G.$$

Nun enthält dieser Ausdruck nicht nur die Zahlen, welche gröfser als 26 und 15 sind, sondern auch alle kleineren, welche der Gleichung

genügen können. Denn nimmt man $F = 2$, $G = 1$ und wendet man das untere Zeichen an, so erhält man:

$$y = 52 - 45 = 7 \text{ und } z = 30 - 26 = 4,$$

und dies ist die Lösung, welche $\frac{26}{15}$ unmittelbar vorausgeht. Setzt man ebenso $n = 2$ oder $F = 7$, $G = 4$ und nimmt man ebenfalls das untere Vorzeichen, so wird:

$$y = 182 - 180 = 2, \quad z = 105 - 104 = 1.$$

Mithin sind sämtliche Lösungen, in grofsen wie in kleinen Zahlen, in gleicher Weise in dem allgemeinen Ausdrucke enthalten, welches auch die besonderen Werte sein mögen, die zur Bildung dieser Formeln verwendet worden sind.

Nachdem dieses festgestellt ist, ist es in keinem Falle notwendig, die gegebene Gleichung

$$fy^2 + gyz + hz^2 = \pm H$$

zu transformieren; man kann sich vielmehr darauf beschränken, den gewöhnlichen, im vorhergehenden Paragraphen angegebenen Weg zu verfolgen. Nachdem man gemäfs dieser Methode eine einzige Wurzel der Gleichung

$$fx^2 + gx + h = 0$$

in einen Kettenbruch entwickelt und die Entwicklung soweit fortgesetzt hat, bis die erste Periode der Quotienten vollständig ist, genügt die Betrachtung dieser ersten Periode, um den allgemeinen Ausdruck der verschiedenen Näherungsbrüche zu erhalten, welche in den aufeinanderfolgenden Perioden der gegebenen Gleichung genügen können. Und man kann sicher sein, dafs die so gefundenen Formeln absolut alle Lösungen enthalten, selbst diejenigen, welche sich, wegen der Unregelmäfsigkeit des Kettenbruchs in seinen ersten Gliedern, nicht unter den ersten Näherungsbrüchen vorfinden.

91.

Um somit die Gleichung

$$1801y^2 - 3991yz + 2211z^2 = -3$$

aufzulösen, entwickle man einfach eine Wurzel der Gleichung

$$1801x^2 - 3991x + 2211 = 0$$

in einen Kettenbruch. Die dazu erforderliche Rechnung, bis dahin fortgesetzt, wo die Wiederkehr desselben vollständigen Quotienten die Ausdehnung der Periode anzeigt, ist folgende:



$$x = \frac{1995\frac{1}{2} + \frac{1}{2}\sqrt{37}}{1801} = 1 + \quad , \qquad 1 : \ \ 0$$

$$\frac{-194\frac{1}{2} + \frac{1}{2}\sqrt{37}}{-21} = 9 + \quad , \qquad 1 : \ \ 1$$

$$\frac{5\frac{1}{2} + \frac{1}{2}\sqrt{37}}{1} = 8 + \quad , \qquad 10 : \ \ 9$$

$$\frac{2\frac{1}{2} + \frac{1}{2}\sqrt{37}}{3} = 1 + \quad , \qquad 81 : \ 73$$

$$\frac{\frac{1}{2} + \frac{1}{2}\sqrt{37}}{3} = 1 + \quad , \qquad 91 : \ 82$$

$$\frac{2\frac{1}{2} + \frac{1}{2}\sqrt{37}}{1} = 5 + \quad , \qquad 172 : 155$$

$$\frac{2\frac{1}{2} + \frac{1}{2}\sqrt{37}}{3} = 1 + \quad , \qquad 951 : 857$$

u. s. w. u. s. w.

Wie man sieht, ist die unaufhörlich sich wiederholende Periode: 1, 1, 5. Wendet man die Formeln des § 9 an, so findet man, dafs die aus dem Bruche $\frac{81}{73}$ sich ergebende Lösung, wenn man

$$(6 + \sqrt{37})^{2k} = F + G\sqrt{37}$$

setzt, die folgende ist:

$$y = 81F \mp 465G$$
$$z = 73F \mp 419G,$$

und die aus dem Bruche $\frac{91}{82}$ sich ergebende Lösung ist, wenn man

$$(6 + \sqrt{37})^{2k+1} = F' + G'\sqrt{37}$$

setzt, die folgende:

$$y = 91F' \mp 577G'$$
$$z = 82F' \mp 520G'.$$

Setzt man in dieser letzteren $F' = 6$ und $G' = 1$, und nimmt man das obere Zeichen, so findet man:

$$y = -31, \quad z = -28.$$

Nun ist es leicht, sich die Gewifsheit zu verschaffen, dafs diese Formeln mit den in No. 89 gefundenen übereinstimmen. Man hat dazu nur an Stelle von F' und G' ihre aus der Gleichung

$$F' + G'\sqrt{37} = (6 \pm \sqrt{37})(F + G\sqrt{37})$$

sich ergebenden Werte, nämlich

$$F' = 6F \pm 37G$$
$$G' = 6G \pm F,$$

einzusetzen.

§ 13.

Weitere Reduktion der Formeln $Ly^2 + Myz + Nz^2$, falls $M^2 - 4LN$ gleich einer positiven Zahl ist.

92.

Wir nehmen zunächst an, dafs der Coefficient M **gerade**, also die gegebene Formel die folgende sei:

$$py^2 + 2qyz + rz^2.$$

In No. 55 haben wir gesehen, dafs, wenn $q^2 - pr$ gleich einer positiven Zahl A ist, diese Formel stets auf die Form

$$ay^2 + 2byz - cz^2$$

gebracht werden kann, in welcher a und c alle beide positiv und nicht kleiner als $2b$ sind, und in der ferner

$$b^2 + ac = A$$

ist. Wir stellen uns jetzt die **Aufgabe**, die verschiedenen Formeln

$$ay^2 + 2byz - cz^2,$$

welche für eine **gegebene** Zahl A den vorhergehenden Bedingungen genügen, **auf die möglich kleinste Anzahl zu reducieren.** Wir zeigen zunächst, wie man zu diesen Formeln kommt.

Ist z. B. $A = 79 = b^2 + ac$, so gebe man b der Reihe nach die Werte 0, 1, 2, 3 und keine andern mehr, da b kleiner sein mufs als $\sqrt{\frac{79}{5}}$. Jeder Wert von b giebt einen Wert von $ac = 79 - b^2$; jedoch ist dieser nur dann brauchbar, wenn er sich in zwei Faktoren, die nicht kleiner als $2b$ sind, zerlegen läfst. Die Einzelheiten der Rechnung, bei welcher beständig $a < c$ vorausgesetzt ist, sind folgende:

1) $\begin{cases} b = 0 \\ ac = 79 \\ a > 0 \end{cases}$ $\quad a = 1, \quad c = 79$

2) $\begin{cases} b = 1 \\ ac = 78 \\ a > 2 \end{cases}$ $\quad \begin{matrix} a = 2, & c = 39 \\ 3 & 26 \\ 6 & 13 \end{matrix}$

$$3)\begin{cases} b = 2 \\ ac = 75 \\ a > 4 \end{cases} \qquad a = 5, \qquad c = 15$$

$$4)\begin{cases} b = 3 \\ ac = 70 \\ a > 6. \end{cases} \qquad a = 7, \qquad c = 10$$

Hieraus ersieht man, dafs sich jede unbestimmte Gröfse

$$py^2 + 2qyz + rz^2,$$

bei welcher

$$q^2 - pr = 79$$

ist, auf eine der zwölf folgenden Formen reducieren mufs:

$$\begin{array}{cc} y^2 - 79z^2 & 79y^2 - z^2 \\ 2y^2 + 2yz - 39z^2 & 39y^2 + 2yz - 2z^2 \\ 3y^2 + 2yz - 26z^2 & 26y^2 + 2yz - 3z^2 \\ 6y^2 + 2yz - 13z^2 & 13y^2 + 2yz - 6z^2 \\ 5y^2 + 4yz - 15z^2 & 15y^2 + 4yz - 5z^2 \\ 7y^2 + 6yz - 10z^2 & 10y^2 + 6yz - 7z^2. \end{array}$$

Von diesen zwölf Formen sind sechs nichts anderes als die andern sechs mit entgegengesetztem Vorzeichen genommen, wobei man noch zu beachten hat, dafs sich die Form $ay^2 + 2byz - cz^2$ von der Form $ay^2 - 2byz - cz^2$ nicht unterscheidet, da man z ohne Unterschied positiv oder negativ nehmen kann.

93.

Es kann der Fall eintreten, dafs eine Formel

$$ay^2 + 2byz - cz^2$$

für gewisse Werte von A mit der zu ihr inversen

$$cy^2 + 2byz - az^2$$

identisch ist, und zwar findet dies immer statt, wenn man der Gleichung $m^2 - An^2 = -1$ genügen kann. Ist nämlich:

$$m^2 - An^2 = -1$$

und setzt man:

$$ay^2 + 2byz - cz^2 = Z = cz'^2 - 2by'z' - ay'^2,$$

so erhält man, wenn man diese beiden Werte von Z, von denen der eine als gegeben, der andere als angenommen betrachtet wird, mit a multipliciert und zur Abkürzung

$$ay + bz = x, \quad ay' + bz' = x'$$

setzt:

$$aZ = x^2 - Az^2$$
$$-aZ = x'^2 - Az'^2,$$

und hieraus folgt wegen $-1 = m^2 - An^2$:

$$x'^2 - Az'^2 = (m^2 - An^2)(x^2 - Az^2).$$

Um dieser Gleichung Genüge zu leisten, kann man sie in die folgenden beiden zerlegen:

$$x' + z'\sqrt{A} = (m - n\sqrt{A})(x + z\sqrt{A})$$
$$x' - z'\sqrt{A} = (m + n\sqrt{A})(x - z\sqrt{A}),$$

aus denen sich ergiebt:

$$x' = mx - nAz$$
$$z' = mz - nx = (m - bn)z - any.$$

Mithin ist zunächst z' eine ganze Zahl; setzt man sodann an Stelle von x und x' ihre Werte $ay + bz$, $ay' + bz'$, so erhält man nach einigen Vereinfachungen:

$$y' = (m + bn)y - cnz.$$

Folglich ist auch y' eine ganze Zahl, und somit ist die Formel $ay^2 + 2byz - cz^2$ dieselbe, wie die zu ihr inverse $cz'^2 - 2by'z' - ay'^2$.

So lange A nicht gröſser ist als 1003, zeigt der Anblick der Tafel X, ob die Gleichung $m^2 - An^2 = -1$ möglich ist; sie ist es stets (No. 43), wenn A eine Primzahl von der Form $4k + 1$ ist, und überhaupt müssen alle Primfaktoren von A oder $\frac{1}{2}A$ von der Form $4k + 1$ sein. Indessen ist diese Bedingung nicht hinreichend, da sie z. B. bei den Zahlen 34, 146, 205 u. s. w. erfüllt ist, ohne daſs die in Rede stehende Gleichung möglich wäre.

94.

Nachdem wir dies vorausgeschickt haben, lassen wir die Methode folgen, vermittelst deren man unter allen zu derselben Zahl A gehörenden Formeln diejenigen auffinden kann, welche mit einer gegebenen Formel $ay^2 + 2byz - cz^2$ identisch sind.

Wenn die Formel

$$Z = ay^2 + 2byz - cz^2$$

mit einer andern Formel

$$a'y'^2 + 2b'y'z' - c'z'^2$$

identisch ist, so mufs diese aus der ersten durch irgend eine Transformation entstehen. Nun besteht die allgemeinste Transformation darin, dafs man setzt (No. 53):

$$y = py' + p^0 z'$$
$$z = qy' + q^0 z',$$

wobei die Zahlen p, q, p^0, q^0 nicht vollständig willkürlich*) sind, sondern der Bedingung

$$pq^0 - p^0 q = \pm 1$$

genügen müssen. Nehmen wir also an, dafs sich durch Einsetzen dieser Werte

$$Z = a'y'^2 + 2b'y'z' - c'z'^2$$

ergebe, so erhalten wir:

$$a' = ap^2 + 2bpq - cq^2$$
$$b' = app^0 + b(pq^0 + p^0 q) - cqq^0$$
$$-c' = ap^{02} + 2bp^0 q^0 - cq^{02}.$$

Will man nun, dafs die Zahlen a' und $-c'$ wirklich von entgegengesetzten Zeichen seien, damit die transformierte Formel der gegebenen ähnlich sei, so mufs eine Wurzel der Gleichung

$$ax^2 + 2bx - c = 0$$

zwischen den beiden Brüchen $\frac{p^0}{q^0}$, $\frac{p}{q}$ liegen. Da ferner

$$b'^2 + a'c' = b^2 + ac = A$$

und somit die eine der Zahlen a' und c' notwendig $< \sqrt{A}$ ist, so mufs wenigstens der eine der beiden vorhergehenden Brüche unter den Näherungsbrüchen der Wurzel x (§ 12) enthalten sein. Ist $\frac{p}{q}$ dieser Bruch und nimmt man für $\frac{p^0}{q^0}$ den Näherungsbruch, welcher $\frac{p}{q}$ vorhergeht, so sind die vier Zahlen p, q, p^0, q^0 durch zwei aufeinanderfolgende Brüche bestimmt, welche sich aus der Entwicklung von x in einen Kettenbruch ergeben. Ich bemerke jedoch, dafs man nicht einmal diese Brüche zu berechnen braucht, um die aufeinanderfolgenden transformierten Formeln $a'y'^2 + 2b'y'z' - c'z'^2$ zu erhalten. Ist nämlich $\frac{\sqrt{A} + J}{D}$ der dem Näherungsbruche $\frac{p}{q}$ entsprechende voll-

---

*) Die Buchstaben p und q stehen zu den Koefficienten der ursprünglichen Form, die wir durch $py^2 + 2qyz + rz^2$ dargestellt hatten, in keiner Beziehung. Anm. d. Verf.

ständige Quotient, so hat man, wie wir oben (No. 59) gefunden haben:

$$ap^2 + 2bpq - cq^2 = D(pq^0 - p^0q)$$
$$app^0 + b(pq^0 + p^0q) - cqq^0 = - J(pq^0 - p^0q)$$
$$ap^{02} + 2bp^0q^0 - cq^{02} = - D^0(pq^0 - p^0q).$$

Mithin wird die transformierte Formel Z einfach:

$$Z = (pq^0 - p^0q)(Dy'^2 - 2Jy'z' - D^0z'^2).$$

Man leitet daher aus jedem vollständigen Quotienten unmittelbar und ohne alle Rechnung die entsprechende transformierte Formel her. Es dürfte überflüssig sein, hinzuzufügen, dafs der Wert des Faktors $pq^0 - p^0q$ bei der ersten transformierten Formel -1, bei der zweiten $+1$ ist, und so abwechselnd weiter.

95.

Suchen wir z. B. die transformierten Formeln, in welche die Formel

$$Z = y^2 - 79z^2$$

übergehen kann, so müssen wir dieselbe Rechnung anstellen, als ob es sich darum handelte, eine Wurzel der Gleichung

$$x^2 - 79 = 0$$

in einen Kettenbruch zu verwandeln. Folgendes ist die hierzu erforderliche Rechnung nebst den daraus sich ergebenden transformierten Formeln:

	Transformierte Formeln:
$x = \sqrt{79} = 8 +$	
$\frac{\sqrt{79}+8}{15} = 1 +$	$-15y^2 + 16yz + z^2$
$\frac{\sqrt{79}+7}{2} = 7 +$	$2y^2 - 14yz - 15z^2$
$\frac{\sqrt{79}+7}{15} = 1 +$	$-15y^2 + 14yz + 2z^2$
$\frac{\sqrt{79}+8}{1} = 16 +$	$y^2 - 16yz - 15z^2$
$\frac{\sqrt{79}+8}{15} = 1 +$	u. s. w.

Man braucht die Rechnung nicht weiter fortzusetzen, da die immer wiederkehrenden nämlichen Quotienten auch zu denselben transformierten Formeln führen. Man sieht also, dafs aus der gegebenen

Formel $y^2 - 79z^2$ nur vier transformierte Formeln entstehen, und diese reducieren sich wieder auf die beiden folgenden:

$$2y^2 - 14yz - 15z^2$$
$$y^2 + 16yz - 15z^2.$$

Bringt man sodann diese auf die gewöhnliche Form, in der $2b < a$ und $< c$ ist, so gehen dieselben über in:

$$2y^2 - 2yz - 39z^2$$
$$y^2 - 79z^2,$$

und da die eine von diesen beiden nichts anderes ist als die gegebene Formel, so giebt es in Wirklichkeit nur eine transformierte Formel derselben, nämlich $2y^2 - 2yz - 39z^2$.

Um die andern Formeln, welche wir für den Fall $A = 79$ gefunden haben (No. 92), zu reducieren, betrachten wir eine von ihnen z. B.

$$3y^2 + 2yz - 26z^2,$$

und entwickeln eine Wurzel der Gleichung

$$3x^2 + 2x - 26 = 0$$

in einen Kettenbruch. Wir finden so die transformierten Formeln:

	Transformierte Formeln:
$x = \frac{-1+\sqrt{79}}{3} = 2 +$	
$\frac{\sqrt{79}+7}{10} = 1 +$	$-10y^2 + 14yz + 3z^2$
$\frac{\sqrt{79}+3}{7} = 1 +$	$7y^2 - 6yz - 10z^2$
$\frac{\sqrt{79}+4}{9} = 1 +$	$-9y^2 + 8yz + 7z^2$
$\frac{\sqrt{79}+5}{6} = 2 +$	$6y^2 - 10yz - 9z^2$
$\frac{\sqrt{79}+7}{5} = 3 +$	$-5y^2 + 14yz + 6z^2$
$\frac{\sqrt{79}+8}{3} = 5 +$	$3y^2 - 16yz - 5z^2$
$\frac{\sqrt{79}+7}{10} =$ u. s. w.	u. s. w.

Bringt man diese sechs transformierten Formeln auf die gewöhnliche Form, so werden dieselben:

$$3y^2 + 2yz - 26z^2$$
$$7y^2 - 6yz - 10z^2$$
$$7y^2 - 6yz - 10z^2$$
$$6y^2 + 2yz - 13z^2$$
$$-5y^2 + 4yz + 15z^2$$
$$3y^2 + 2yz - 26z^2.$$

Hieraus geht hervor, dafs die oben für die unbestimmte Gröfse $py^2 + 2qyz + rz^2$ im Falle $q^2 - pr = 79$ gefundenen zwölf Formen sich auf folgende vier reducieren:

$$y^2 - 79z^2 \qquad\qquad 79y^2 - z^2$$
$$3y^2 + 2yz - 26z^2 \qquad\qquad 26y^2 - 2yz - 3z^2.$$

Mithin kann jede Gleichung von der Form:

$$py^2 + 2qyz + rz^2 = \pm H,$$

bei welcher

$$q^2 - pr = 79$$

ist, stets auf eine der beiden Gleichungen

$$y^2 - 79z^2 = \pm H$$
$$3y^2 + 2yz - 26z^2 = \pm H$$

zurückgeführt werden.

§ 96.

Nach diesen Principien ist die Tafel I konstruiert worden. In derselben findet man für jede nichtquadratische Zahl A von 2 bis 136 die verschiedenen Hauptformen, auf welche sich die unbestimmten Formeln $Ly^2 + 2Myz + Nz^2$, in denen $M^2 - LN = A$ ist, stets reducieren lassen. Die Zeichen $\pm$, mit denen die meisten Formeln behaftet sind, zeigen zwei Formen an, die in gleicher Weise möglich sind, sich aber gegenseitig ausschliefsen. Sind die Formeln nicht mit dem Doppelzeichen versehen, so gelten sie so, wie sie angegeben sind, doch würden sie mit entgegengesetztem Vorzeichen ebenfalls stattfinden.

So findet man z. B. neben der Zahl 93 die reducierte Formel $\pm(y^2 - 93z^2)$. Dies bedeutet, dafs jede gegebene Formel

$$py^2 + 2qyz + rz^2,$$

in welcher $q^2 - pr = 93$ ist, sich stets auf die Form $y'^2 - 93z'^2$ oder auf die Form $93z'^2 - y'^2$, niemals aber auf beide Formen zugleich bringen läfst.

Dagegen findet man neben der Zahl 97 die Formel $y^2 - 97z^2$ ohne Doppelzeichen. Dies bedeutet, dafs jede gegebene Formel

$$py^2 + 2qyz + rz^2,$$

in welcher $q^2 - pr = 97$ ist, sich stets auf die Form $y'^2 - 97z'^2$ bringen läfst. Sie kann aber, wenn man will, auch auf die Form $97z'^2 - y'^2$ gebracht werden, da man in diesem Falle der Gleichung $m^2 - 97n^2 = -1$ genügen kann.

97.

Wir betrachten jetzt die unbestimmte Formel:

$$Ly^2 + Myz + Nz^2,$$

in welcher M eine **ungerade** Zahl und die Gröfse $M^2 - 4LN$ gleich einer **positiven** Zahl B ist. Diese Formel läfst sich stets auf die Form bringen:

$$ay^2 + byz - cz^2,$$

in welcher zu gleicher Zeit a und c positiv, $b < a$ und $< c$ und $b^2 + 4ac = B$ ist. Mittelst der einen, als bekannt vorausgesetzten Zahl B kann man leicht alle Formeln $ay^2 + byz - cz^2$ finden, welche den vorstehenden Bedingungen genügen; sodann aber handelt es sich darum, diese Formeln **auf die geringste Anzahl zu reducieren,** indem man die überflüssigen oder in den andern enthaltenen Formeln wegläfst.

Dazu betrachten wir eine von diesen Formeln:

$$ay^2 + byz - cz^2,$$

oder vielmehr das Doppelte derselben:

$$2ay^2 + 2byz - 2cz^2.$$

Da alsdann der Koefficient des mittleren Gliedes gerade ist, so kann man auf demselben Wege wie vorher zur Aufsuchung der aufeinanderfolgenden Transformationen derselben schreiten. Zu dem Zwecke mufs man eine Wurzel der Gleichung

$$2ax^2 + 2bx - 2c = 0$$

in einen Kettenbruch entwickeln. Diese Wurzel sei $x = \frac{-b + \sqrt{B}}{2a}$. Die transformierten Formeln sind ebenfalls von der Form:

$$2a'y^2 + 2b'yz - 2c'z^2,$$

die sich stets aus dem Ausdruck

$$(pq^0 - p^0q)(Dy^2 - 2Jyz - D^0z^2)$$

ergiebt. Dabei ist der allen gemeinsame Faktor 2 nicht hinderlich, um mit gleicher Leichtigkeit die identischen Formen zu erkennen.

In Wahrheit giebt es also keinen wesentlichen Unterschied zwischen der Art der Behandlung des Falles, wo M gerade, und desjenigen, wo M ungerade ist. Indessen müssen die Resultate dieses letzteren Falles in einer besonderen Tafel verzeichnet werden, welche für jede Zahl B von der Form $4n + 1$ die wesentlich verschiedenen Formen angiebt, auf welche sich alle unbestimmten Formeln $Ly^2 + Myz + Nz^2$, in denen M ungerade und $M^2 - 4LN = B$ ist, zurückführen lassen.

98.

Um von der Berechnung dieser Tafel ein Beispiel zu geben, sei $B = 181$. Wir suchen zunächst die verschiedenen Werte von a, b, c, welche der Gleichung

$$b^2 + 4ac = 181$$

genügen, und da den andern Bedingungen zufolge die ungerade Zahl b kleiner als $\sqrt{\frac{181}{5}}$ sein mufs, so setzen wir der Reihe nach $b = 1, 3, 5$. Dies giebt, wenn wir $a < c$ annehmen:

$$1) \begin{cases} b = 1 & a = 1, \quad c = 45 \\ ac = 45 & \phantom{a = {}} 3, \quad \phantom{c = {}} 15 \\ a > 1 & \phantom{a = {}} 5, \quad \phantom{c = {}} 9 \end{cases}$$

$$2) \begin{cases} b = 3 \\ ac = 43\text{: nicht zerlegbar} \\ a > 3 \end{cases}$$

$$3) \begin{cases} b = 5 \\ ac = 39\text{: nicht zerlegbar in Faktoren, die gröfser als 5 sind.} \\ a > 5. \end{cases}$$

Mithin lassen sich die unbestimmten Formeln $Ly^2 + Myz + Nz^2$, in denen

$$M^2 - 4LN = 181$$

ist, sämtlich auf eine von den folgenden sechs Formen zurückführen:

$$\pm (y^2 + yz - 45z^2)$$
$$\pm (3y^2 + yz - 15z^2)$$
$$\pm (5y^2 + yz - 9z^2).$$

Da übrigens 181 eine Primzahl von der Form $4n + 1$ ist, so ist die Gleichung $m^2 - 181n^2 = -1$ möglich (No. 43); somit reducieren sich, wenn man das Doppelzeichen wegläfst, die vorhergehenden sechs Formen auf drei. Es bleibt also nur zu untersuchen, ob diese drei Formen sich auf eine geringere Anzahl reducieren.

Dazu suchen wir die transformierten Formeln zu $2y^2+2yz-90z^2$, indem wir eine Wurzel der Gleichung $2x^2+2x-90=0$ durch folgende Rechnung in einen Kettenbruch entwickeln:

	Transformierte Formeln.
$x=\frac{-1+\sqrt{181}}{2}=6+$	
$\frac{13+\sqrt{181}}{6}=4+$	$-6y^2+26yz+2z^2$
$\frac{11+\sqrt{181}}{10}=2+$	$10y^2+22yz-6z^2$
$\frac{9+\sqrt{181}}{10}=2+$	$-10y^2+18yz+10z^2$
$\frac{11+\sqrt{181}}{6}=4+$	$6y^2+22yz-10z^2$
$\frac{13+\sqrt{181}}{2}=13+$	$-2y^2+26yz+6z^2$
$\frac{13+\sqrt{181}}{6}=4+$	$6y^2+26yz-2z^2$
u. s. w.	u. s. w.

Hierauf mufs man diese transformierten Formeln durch 2 dividieren und dieselben durch Verkleinerung des mittleren Koefficienten auf die gewöhnliche Form bringen. Ich bemerke nun, dafs dies auf zweierlei Weise geschehen kann, sobald dieser Koefficient gröfser als jeder der beiden äufseren ist. Z. B. kann man in der transformierten Formel

$$-3y^2+13yz+z^2$$

an Stelle von y setzen: $y+2z$; dies giebt:

$$-3y^2+yz+15z^2;$$

oder man kann $z-6y$ an Stelle von z setzen, und dies giebt:

$$z^2+yz-45y^2.$$

Behandelt man ebenso die beiden ersten transformierten Formeln, und beachtet man, dafs es wegen der besonderen Beschaffenheit der Zahl 181 gestattet ist, in jedem Resultat sämtliche Vorzeichen zu ändern, so findet man, dafs sie allein folgende drei Formen in sich enthalten:

$$y^2+yz-45z^2$$
$$3y^2-yz-15z^2$$
$$5y^2+yz-9z^2.$$

Man braucht daher nicht erst die andern transformierten Formeln zu berücksichtigen, vielmehr ist man sicher, dafs die einzige Form

$$y^2+yz-45z^2$$

alle übrigen in sich faſst. Mithin läſst sich jede unbestimmte Gleichung in welcher

$$Ly^2 + Myz + Nz^2 = \pm H,$$
$$M^2 - 4LN = 181$$

ist, stets auf die Form

$$y^2 + yz - 45z^2 = H$$

zurückführen.

99.

Die Tafel II giebt die Reduktionen dieser Art für alle Zahlen B von der Form $4n + 1$ von 5 bis 305. Diese Tafel kann, unabhängig von ihrem sonstigen Gebrauch, die Auflösung der Gleichungen von der eben erwähnten Form, in denen B die Zahl 305 nicht übersteigt, bedeutend erleichtern.

Es dürfte vielleicht nicht unnützlich sein, an einem Beispiele zu zeigen, wie man diese Reduktionen in den besonderen Fällen wirklich ausführt.

Es sei die Gleichung gegeben:

$$333y^2 - 719yz + 388z^2 = H.$$

Um durch eine einfache Rechnung die Transformation der linken Seite zu erhalten, entwickeln wir eine Wurzel der Gleichung

$$333x^2 - 719x + 388 = 0$$

in einen Kettenbruch und berechnen zugleich die daraus sich ergebenden Näherungsbrüche. Folgendes sind die Einzelheiten der Rechnung, die man bloſs soweit fortzusetzen brauchte, bis die vollständigen Quotienten aufhören, irregulär zu sein, die wir aber durch eine ganze Periode hindurch ausgeführt haben, da diese Periode nur aus drei Gliedern besteht.

$x = \frac{719 + \sqrt{145}}{666} = 1 +$	1 : 0
$\frac{-53 + \sqrt{145}}{-4} = 10 +$	1 : 1
$\frac{13 + \sqrt{145}}{6} = 4 +$	11 : 10
$\frac{11 + \sqrt{145}}{4} = 5 +$	45 : 41
$\frac{9 + \sqrt{145}}{16} = 1 +$	u. s. w.
$\frac{7 + \sqrt{145}}{6} = 3 +$	
$\frac{11 + \sqrt{145}}{4} = 5 +$	

Hieraus und aus den Artikeln 94 und 97 folgt, dafs man, wenn man

$$y = 45y' + 11z'$$
$$z = 41y' + 10z'$$

setzt, als Transformation der linken Seite erhält:

$$-(2y'^2 - 11y'z' - 3z'^2).$$

Diese transformierte Formel ist noch nicht auf die geeignete Form gebracht; man mufs, damit der mittlere Koefficient nicht gröfser als die beiden äufseren sei,

$$y' = u' + 3z'$$

annehmen. Dies giebt:

$$-2u'^2 - u'z' + 18z'^2.$$

Man mufs demnach setzen:

$$y = 45u' + 146z'$$
$$z = 41u' + 133z'.$$

Alsdann ist die aus der gegebenen Gleichung durch Transformation hervorgegangene Gleichung in ihrer einfachsten Form folgende:

$$2u'^2 + u'z' - 18z'^2 = -H.$$

§ 14.

Entwicklung der reellen Wurzel einer Gleichung beliebigen Grades in einen Kettenbruch.

100.

Es sei die **Aufgabe** gestellt, **eine reelle Wurzel der Gleichung**

$$ax^n + bx^{n-1} + cx^{n-2} + \cdots + k = 0,$$

deren Koefficienten ganze, positive oder negative, Zahlen sind, **in einen Kettenbruch zu entwickeln.**

Zunächst kann man annehmen, dafs diese Gleichung durch **keinen rationalen Faktor** teilbar ist; denn im andern Falle könnte man den Faktor, der mit der zu entwickelnden Wurzel nichts zu thun hat, unterdrücken, wodurch die Rechnung bedeutend einfacher werden würde. Aus demselben Grunde kann die gegebene Gleichung **keine gleichen Wurzeln** haben; denn hätte sie solche, so würde sie durch einen rationalen Faktor, der sich nach den bekannten Methoden leicht finden liefse, teilbar sein.

Dies vorausgeschickt, wird die betreffende, unter allen andern ausgewählte Wurzel wenigstens bis auf eine Einheit bekannt sein.

Ist α die kleinere der beiden benachbarten ganzen Zahlen, zwischen denen sie enthalten ist, so setze man,

wenn x positiv ist, $x = \alpha + \frac{1}{x'}$

wenn x negativ ist, $x = -\alpha - \frac{1}{x'}$.

Alsdann ist man sicher, dafs der Wert von x' positiv und gröfser als 1 ist. Setzt man diesen Wert in die gegebene Gleichung ein, so erhält man die transformierte Gleichung:

$$a'x'^n + b'x'^{n-1} + c'x'^{n-2} + \cdots + k' = 0,$$

welche zur Bestimmung von x' dient. Nun weifs man bereits, dafs der Wert von x', dessen man bedarf, positiv und gröfser als 1 ist; es kann sogar mehrere Werte von x' geben, welche diese Bedingungen erfüllen, da es mehrere Wurzeln der gegebenen Gleichung geben kann, welche, ohne gleich zu sein, zwischen α und $\alpha + 1$ enthalten sind. Man versuche demnach für x' der Reihe nach die Zahlen 1, 2, 3 u. s. w., bis man nach den bekannten Kennzeichen die nächsten ganzen Zahlen, zwischen denen der Wert von x' liegt, findet. Ist β die kleinere der beiden, so setze man:

$$x' = \beta + \frac{1}{x''},$$

und substituiere diesen Wert in die Gleichung für x'. Dadurch erhält man zur Bestimmung von x'' eine neue transformierte Gleichung:

$$a''x''^n + b''x''^{n-1} + \cdots + k'' = 0,$$

die man ebenso wie die vorhergehende behandelt. Indem man in dieser Weise, soweit man will, fortfährt, wird der Wert von x offenbar durch folgenden Kettenbruch ausgedrückt werden:

$$x = \alpha + \cfrac{1}{\beta + \cfrac{1}{\gamma + \cdots}}$$

Mit Hülfe dieser bekannten Quotienten berechnet man dann wie gewöhnlich die Näherungsbrüche von x.

101.

Sind $\frac{p^0}{q^0}$, $\frac{p}{q}$ zwei von diesen aufeinanderfolgenden Brüchen, und ist z der dem letzteren entsprechende vollständige Quotient, so hat man der bekannten Eigenschaft zufolge:

$$x = \frac{pz + p^0}{qz + q^0}.$$

Man kann somit direkt eine beliebige transformierte Gleichung finden, indem man diesen Wert an Stelle von x in die gegebene Gleichung einsetzt. Ist

$$Az^n + Bz^{n-1} + Cz^{n-2} + \cdots + K = 0$$

diese transformierte Gleichung, so erhält man:

$$A = ap^n + bp^{n-1}q + cp^{n-2}q^2 + \cdots + kq^n$$
$$K = ap^{0n} + bp^{0n-1}q^0 + cp^{0n-2}q^{0\,2} + \cdots + kq^{0n},$$

so dafs nach unsern gewöhnlichen Bezeichnungen allgemein sein würde:

$$K = A^0, \quad \text{oder } K' = A.$$

Es ist indessen viel einfacher, nach und nach jede transformierte Gleichung auf die bereits auseinandergesetzte Weise aus der vorhergehenden transformierten Gleichung abzuleiten. Um in dieser Hinsicht die Rechnung möglichst einfach zu machen, bemerken wir, dafs sich, wenn man

$$z = \mu + \frac{1}{z'}$$

setzt und dadurch die vorhergehende Gleichung in die folgende

$$A'z'^n + B'z'^{n-1} + C'z'^{n-2} + \cdots + K' = 0$$

übergeht, die nachstehenden Gleichungen ergeben:

$$A' = A\mu^n + B\mu^{n-1} + C\mu^{n-2} + \cdots + K$$
$$B' = nA\mu^{n-1} + (n-1)B\mu^{n-2} + (n-2)C\mu^{n-3} + \cdots$$
$$C' = \frac{n(n-1)}{2} A\mu^{n-2} + \frac{(n-1)(n-2)}{2} B\mu^{n-3} + \cdots$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$K' = A.$$

Bezeichnet man demnach die Funktion

$$Az^n + Bz^{n-1} + Cz^{n-2} + \cdots + K$$

mit $\varphi(z)$ oder φ, bildet sodann durch Differentiation nach und nach die Gröfsen:

$$\varphi, \frac{d\varphi}{dz}, \frac{d^2\varphi}{2dz^2}, \frac{d^3\varphi}{2\cdot 3dz^3}, \cdots$$

und setzt darauf an Stelle von z den angenäherten Wert μ ein, so geben diese Gröfsen bezüglich die Werte der Koefficienten $A', B', C', \cdots$ in der folgenden transformierten Gleichung.

Dies ist die Methode, welche zuerst Lagrange für die Entwicklung der Wurzeln der Gleichungen in einen Kettenbruch angegeben hat. Indessen würde diese Methode in der Praxis von

abschreckender Länge sein, wenn nicht derselbe Autor ein sehr einfaches Mittel angegeben hätte, wie man, ohne zu probieren, die Reihe der ganzen Zahlen $\alpha, \beta, \gamma, \delta \ldots$ fortsetzen kann, sobald einige der ersten Glieder bereits bekannt sind. Diese Vervollkommnung besteht in Folgendem.

102.

Die Formel

$$x = \frac{pz + p^0}{qz + q^0}$$

giebt:

$$z = \frac{q^0 x - p^0}{p - qx},$$

oder:

$$z + \frac{q^0}{q} = \frac{pq^0 - p^0 q}{q(p - qx)}.$$

Bezeichnen wir stets mit x die Wurzel, welche man entwickeln will, mit $x_1, x_2, x_3, \ldots$ die andern Wurzeln der gegebenen Gleichung und mit $z_1, z_2, z_3, \ldots$ die entsprechenden Werte von z, so hat man aufser der vorhergehenden Gleichung noch die $n - 1$ folgenden:

$$z_1 + \frac{q^0}{q} = \frac{pq^0 - p^0 q}{q(p - qx_1)}$$

$$z_2 + \frac{q^0}{q} = \frac{pq^0 - p^0 q}{q(p - qx_2)}$$

$$z_3 + \frac{q^0}{q} = \frac{pq^0 - p^0 q}{q(p - qx_3)}$$

u. s. w.

Addieren wir alle diese Gleichungen und beachten wir, dafs, da die Gleichung in z ist: $Az^n + Bz^{n-1} + \cdots = 0$, man erhält:

$$z + z_1 + z_2 + z_3 + \cdots = -\frac{B}{A},$$

so ergiebt sich als Summe:

$$-z - \frac{B}{A} + (n-1)\frac{q^0}{q} = (pq^0 - p^0 q)\frac{\Delta}{q^2} = \pm \frac{\Delta}{q^2},$$

wo zur Abkürzung

$$\Delta = \frac{1}{\frac{p}{q} - x_1} + \frac{1}{\frac{p}{q} - x_2} + \frac{1}{\frac{p}{q} - x_3} + \cdots$$

gesetzt ist.

Ist nun die Zahlgröfse $\frac{\Delta}{q^2}$ hinreichend klein, um vernachlässigt werden zu können, so wird offenbar der Wert von x auf direkte Weise und ohne alles Probieren durch die Formel

$$z = (n-1)\frac{q^0}{q} - \frac{B}{A}$$

gegeben sein. Man mufs somit für μ die gröfste in diesem Werte enthaltene ganze Zahl nehmen; dieses μ ist dann der dem Näherungsbruche $\frac{p}{q}$ entsprechende Quotient. Hit Hülfe dieses Quotienten berechnet man sodann den folgenden Bruch $\frac{p'}{q'}$ und die folgende transformierte Gleichung für z', so dafs man also die Rechnung, soweit man will, ohne alles Probieren fortsetzen kann.

103.

Die Gröfse Δ ändert sich mit den verschiedenen Brüchen $\frac{p}{q}$, auf die sie sich bezieht; sie kann aber nicht unendlich grofs werden, da sonst ein Nenner z. B. $\frac{p}{q} - x_1$ gleich Null sein müfste und somit die gegebene Gleichung einen rationalen Teiler $p - qx$ hätte, was gegen die Voraussetzung ist.

Jedoch kann diese Gröfse Δ zuweilen sehr beträchtlich sein, und zwar wird dies stattfinden, wenn zwischen der Wurzel x und einer oder mehreren der andern Wurzeln $x_1, x_2, \ldots$ nur ein geringer Unterschied stattfindet. Da sich übrigens die Näherungsbrüche $\frac{p}{q}$ sehr schnell dem Werte von x nähern, so werden sich offenbar die Gröfsen Δ nicht weniger schnell der Grenze

$$T = \frac{1}{x - x_1} + \frac{1}{x - x_2} + \frac{1}{x - x_3} + \cdots$$

nähern. Setzt man also die Berechnung der Glieder des Kettenbruches und die der Näherungsbrüche nach der ersten Methode soweit fort, bis $\frac{T}{q^2}$ kleiner ist als ein bestimmter Bruch $\frac{1}{m}$, oder bis man

$$q > \sqrt{Tm}$$

hat (wobei T positiv genommen ist), so ist klar, dafs der oben gefundene Wert von z nämlich:

$$z = (n - 1)\frac{q^0}{q} - \frac{B}{A}$$

nur um eine Gröfse, die kleiner als $\frac{1}{m}$ ist, fehlerhaft ist. Mithin reicht schon eine ziemlich unvollkommene Kenntnis der Wurzeln der gegebenen Gleichung, ja sogar allein die Kenntnis derjenigen, welche nur wenig von der zu entwickelnden Wurzel verschieden sind, aus zur Bestimmung der Grenze, nach welcher man die Rechnung mit Hülfe der vorhergehenden Formel ohne alles Probieren fortsetzen kann.

Zu diesen von der gegebenen nur wenig verschiedenen Wurzeln mufs man auch die imaginären Wurzeln hinzunehmen. Denn analytisch ausgedrückt ist eine Wurzel $\alpha + \beta\sqrt{-1}$, in welcher $\frac{\beta}{\alpha}$ sehr klein ist, als nur wenig von α verschieden zu betrachten. Hat man daher eine imaginäre Wurzel $x_1 = \alpha + \beta\sqrt{-1}$ und demnach noch eine zweite $x_2 = \alpha - \beta\sqrt{-1}$, so ergeben sich aus diesen beiden Wurzeln, wenn man sie in den Wert von T einsetzt, die beiden Glieder:

$$\frac{1}{x - \alpha - \beta\sqrt{-1}} + \frac{1}{x - \alpha + \beta\sqrt{-1}},$$

und diese reducieren sich auf die reelle Gröfse:

$$\frac{2(x-\alpha)}{(x-\alpha)^2 + \beta^2}.$$

Diese Gröfse kann das Maximum $\frac{1}{\beta}$ nicht überschreiten; jedoch kann sie noch ziemlich grofs sein, wenn β und ebenso $x - \alpha$ sehr klein ist.

Wenn die Differenz zwischen der Wurzel x und jeder der andern Wurzeln (diese Differenz verwandelt sich in die Summe, wenn die beiden Wurzeln entgegengesetztes Zeichen haben) gröfser als 1 ist, dann ist offenbar T kleiner als $n - 1$, und die Grenze von q ist:

$$q > \sqrt{(n-1)m},$$

also ein ziemlich kleiner Wert. Sonach kann man von der Formel fast vom Beginn der Rechnung an Gebrauch machen und hat alsdann fast gar nicht zu probieren.

Wenn dagegen die Wurzel x nur wenig von einer oder mehreren reellen oder imaginären Wurzeln der gegebenen Gleichung verschieden ist, so mufs man die erste Methode bei einer gewissen Anzahl von Gliedern anwenden; indessen wird man bald die Grenze $q > \sqrt{Tm}$ erreichen, wonach man die Rechnung ohne das geringste Probieren fortsetzen kann. Man kann übrigens bemerken, dafs, im Falle es wirklich zwei oder mehrere wenig von einander verschiedene Wurzeln giebt, die Gleichung

$$nax^{n-1} + (n-1)bx^{n-2} + (n-2)cx^{n-3} + \cdots = 0,$$

welche beim Vorhandensein von gleichen Wurzeln gilt, wenigstens annähernd auch dann richtig ist, wenn nur wenig von einander verschiedene Wurzeln vorhanden sind. Dies kann zur Auffindung der ersten Ziffern dieser Wurzeln von Vorteil sein.

104.

Wenn die Operation der Entwicklung bis zu einem gewissen Punkte fortgeschritten ist, und die Nenner q der Näherungsbrüche anfangen etwas grofs zu werden, so giebt die Formel

$$z = (n-1)\frac{q^0}{q} - \frac{B}{A}$$

nicht allein den Quotienten μ, welcher dem Bruche $\frac{p}{q}$ entspricht, sondern man kann auch, wenn man diesen Wert von z in einen Kettenbruch entwickelt, die aus dieser Entwicklung sich ergebenden Quotienten den bereits gefundenen Quotienten anreihen. Dieselben sind genau bis auf eine Grenze, die wir jetzt bestimmen wollen.

Da der genaue Wert von z

$$z = (n-1)\frac{q^0}{q} - \frac{B}{A} \pm \frac{\Delta}{q^2}$$

ist, so veranlafst die Vernachlässigung des Gliedes $\frac{\Delta}{q^2}$ einen Fehler in x, welcher durch die strenge Gleichung

$$p - qx = \frac{\pm 1}{qz + q^0},$$

gegeben wird, wenn man darin $z \pm \frac{\Delta}{q^2}$ an Stelle von z und $x + \delta x$ an Stelle von x setzt. Man findet so:

$$\delta x = \frac{\Delta}{q^2(qz + q^0)^2}.$$

Sind $\mu, \mu', \mu'', \ldots \omega$ die Quotienten, welche aus der Entwicklung der Gröfse $(n-1)\frac{q^0}{q} - \frac{B}{A}$ sich ergeben, und nimmt man an, dafs man, wenn man mittelst dieser Quotienten die Berechnung der Näherungsbrüche von x fortsetzt, zu dem Bruche $\frac{P}{Q}$ gelange, so wird dieser letztere ebenfalls (No. 9) ein Näherungsbruch sein, wenn man hat:

$$\frac{P}{Q} - x < \frac{1}{2Q^2}.$$

Sobald daher

$$\frac{1}{Q^2} > \frac{2\Delta}{q^2(qz + q^0)^2}$$

oder

$$Q < \frac{q(qz + q^0)}{\sqrt{2\Delta}}$$

oder ungefähr

$$Q < \frac{q^2\mu}{\sqrt{2T}}$$

ist, wird der Bruch $\frac{P}{Q}$ ebenfalls einer der Näherungsbrüche von x

sein. Geht man demnach von dem Näherungsbruche $\frac{p}{q}$ aus, so liefert der entsprechende Wert von z, in einen Kettenbruch entwickelt, die Quotienten, welche notwendig sind, um die Näherungsbrüche von x soweit fortzusetzen, bis sie ungefähr doppelt so viel Ziffern haben wie der, von dem man ausgegangen ist.

105.

Beispiel 1.

Es sei die Gleichung

$$x^3 - x^2 - 2x + 1 = 0$$

gegeben, deren Wurzeln bekanntlich

$$x = 2 \cos \frac{1}{7}\pi, \quad x = -2 \cos \frac{2}{7}\pi, \quad x = 2 \cos \frac{3}{7}\pi$$

sind, wo π der halbe Umfang eines Kreises mit dem Radius 1 ist. Man hat also nahezu:

$$x = 1{,}802, \quad x = -1{,}247, \quad x = 0{,}445.$$

Um zunächst die erste Wurzel zu entwickeln, beachte man, dafs man, da die Differenzen zwischen dieser Wurzel und den beiden andern

$$x - x_1 = 3{,}049 \text{ und } x - x_2 = 1{,}357$$

sind, die Grenze erhält:

$$T = \frac{1}{3{,}049} + \frac{1}{1{,}357} = 1 \text{ (ungefähr)}.$$

Mithin wird die Formel, welche den Wert von z giebt, mindestens bis auf $\frac{1}{10}$ genau sein, wenn $q > \sqrt{10}$ oder $q > 3$ ist, und mindestens bis auf $\frac{1}{100}$ genau, wenn $q > 10$ ist. Es giebt also in diesem Falle gar kein Probieren. Im Übrigen sind die Einzelheiten der Rechnung folgende.

Da der Wert von x, den man entwickeln will, zwischen 1 und 2 liegt, so setze man:

$$x = 1 + \frac{1}{z}.$$

Dadurch erhält man die transformierte Gleichung:

$$-z^3 - z^2 + 2z + 1 = 0.$$

Bei dieser erkennt man leicht, dafs der positive Wert von z ebenfalls zwischen 1 und 2 liegt. Man setze also $z = 1 + \frac{1}{z'}$ oder einfach $1 + \frac{1}{z}$ an Stelle von z; denn es ist unnötig, die Unbekannten der aufeinanderfolgenden transformierten Gleichungen durch Striche



von einander zu unterscheiden; man weifs, dafs sie verschieden sein müssen. Die transformierte Gleichung wird also:

$$z^3 - 3z^2 - 4z - 1 = 0.$$

In dieser letzteren liegt der Wert von z zwischen 4 und 5, so dafs man $4 + \frac{1}{z}$ an die Stelle von z zu setzen hat. Um jedoch diese Substitution nach der in No. 101 angegebenen Methode auszuführen, bilde ich der Reihe nach die Gröfsen:

$$\varphi = z^3 - 3z^2 - 4z - 1$$

$$\frac{d\varphi}{dz} = 3z^2 - 6z - 4$$

$$\frac{d^2\varphi}{2 \cdot dz^2} = 3z - 3$$

$$\frac{d^3\varphi}{2 \cdot 3 dz^3} = 1.$$

Darauf setze ich in diese Gröfsen den Wert $z = 4$ ein und erhalte die vier Zahlen -1, 20, 9, 1, wonach sich folgende transformierte Gleichung ergiebt:

$$-z^3 + 20z^2 + 9z + 1 = 0.$$

Jetzt ist die Rechnung weit genug vorgeschritten, um ohne Probieren fortgesetzt werden zu können. Zunächst bilden wir mit Hülfe der gefundenen Quotienten 1, 1, 4 die Näherungsbrüche, wie folgt:

Quotienten; 1, 1, 4

Näherungsbrüche: $\frac{1}{0}$, $\frac{1}{1}$, $\frac{2}{1}$, $\frac{9}{5}$.

Die durch die letzte transformierte Gleichung bestimmte Gröfse z ist der dem Bruche $\frac{9}{5}$ entsprechende vollständige Quotient. Der Formel

$$z = \frac{2q^0}{q} - \frac{B}{A}$$

zufolge hat man aber:

$$z = \frac{2}{5} + 20.$$

Mithin ist 20 die gröfste in z enthaltene ganze Zahl. Mittelst dieses neuen Quotienten 20 kann man die Berechnung der Näherungsbrüche um ein Glied weiter fortsetzen, nämlich:

$$1, \quad 1, \quad 4, \quad 20$$

$$\frac{1}{0}, \quad \frac{1}{1}, \quad \frac{2}{1}, \quad \frac{9}{5}, \quad \frac{182}{101}.$$

Um die folgende transformierte Gleichung zu erhalten, bildet man die vier Gröfsen:

$$\varphi = - z^3 + 20z^2 + 9z + 1$$
$$\frac{d\varphi}{dz} = - 3z^2 + 40z + 9$$
$$\frac{d^2\varphi}{2\,dz^2} = - 3z + 20$$
$$\frac{d^3\varphi}{2\cdot 3\,dz^3} = - 1,$$

und setzt darin den Wert $z = 20$ ein. Dies giebt die vier Zahlen 181, $-$ 391, $-$ 40, $-$ 1, und demnach wird die neue transformierte Gleichung:

$$181z^3 - 391z^2 - 40z - 1 = 0.$$

Der angenäherte Wert von z in dieser transformierten Gleichung ist zufolge unserer Formel:

$$z = \frac{10}{101} + \frac{391}{181} = 2 +;$$

mithin ist 2 der nächstfolgende Quotient. Indem man so weitergeht, findet man die in folgendem Schema niedergelegten Resultate:

Entwicklung der zwischen 1 und 2 liegenden Wurzel.

Gegebene Gleichung und die aufeinanderfolgenden transformierten Gleichungen.	In der Wurzel enthaltene gröfste ganze Zahl.	Näherungs-brüche.
$x^3 - x^2 - 2x + 1 = 0$	1	1 : 0
$- z^3 - z^2 + 2z + 1 = 0$	1	1 : 1
$z^3 - 3z^2 - 4z - 1 = 0$	4	2 : 1
$- z^3 + 20z^2 + 9z + 1 = 0$	20	9 : 5
$181z^3 - 391z^2 - 40z - 1 = 0$	2	182 : 101
$- 197z^3 + 568z^2 + 695z + 181 = 0$	3	373 : 207
$2059z^3 - 1216z^2 - 1205z - 197 = 0$	1	1301 : 722
$- 559z^3 + 2540z^2 + 4961z + 2059 = 0$	6	1674 : 929
$2521z^3 - 24931z^2 - 7522z - 559 = 0$	10	11345 : 6296
$- 47879z^3 + 250158z^2 + 50699z + 2521 = 0$		115124 : 63889
u. s. w.		u. s. w.

Die letzte transformierte Gleichung hat zur Wurzel näherungsweise:

$$z = \frac{12592}{63889} + \frac{250158}{47879},$$

und diese Gröfse giebt, in einen einzigen Bruch verwandelt und in einen Kettenbruch entwickelt, die Quotienten 5, 2, 2, 1, 2, 2, 1, 18, 1, 1, 3 ... Man kann also mit Hülfe dieser den bereits gefundenen Quotienten anzureihenden Quotienten die Berechnung der Näherungsbrüche fortsetzen, bis ihre Zähler und Nenner 11 oder 12 Ziffern haben. Durch ähnliche Rechnungen entwickelt man die beiden andern Wurzeln, wie man aus den beiden folgenden Schematen sieht:

Entwicklung der zwischen 0 und 1 liegenden Wurzel.

Gegebene Gleichung und transformierte Gleichungen.	In der Wurzel enthaltene gröfste ganze Zahl.	Näherungsbrüche.
$x^3 - x^2 - 2x + 1 = 0$	0	1 : 0
$z^3 - 2z^2 - z + 1 = 0$	2	0 : 1
$-z^3 + 3z^2 + 4z + 1 = 0$	4	1 : 2
$z^3 - 20z^2 - 9z - 1 = 0$	20	4 : 9
Folgen dieselben transformierten Gleichungen und folglich dieselben Quotienten wie bei der Entwicklung der ersten Wurzel.	2	81 : 182
	3	166 : 373
	1	579 : 1301
	6	745 : 1674
	10	5049 : 11345
	5	51235 : 115124
	2	261224 : 586965
	u. s. w.	u. s. w.

Entwicklung der zwischen — 1 und — 2 liegenden Wurzel.

$x^3 - x^2 - 2x + 1 = 0$	— 1	— 1 : 0
$z^3 - 3z^2 - 4z - 1 = 0$	4	— 1 : 1
$-z^3 + 20z^2 + 9z + 1 = 0$	20	— 5 : 4
Folgen ebenfalls dieselben transformierten Gleichungen und dieselben Quotienten, die man bei der Entwicklung der ersten Wurzel gefunden hatte.	2	— 101 : 81
	3	— 207 : 166
	1	— 722 : 579
	6	— 929 : 745
	10	— 6296 : 5049
	5	— 63889 : 51235
	u. s. w.	u. s. w.

Bei diesem Beispiel ist sehr bemerkenswert, dafs man eine

Beziehung zwischen den drei Wurzeln findet, vermöge deren die Entwicklung der ersten Wurzel genügt, um auch die der beiden andern zu geben. Diese Beziehung ist derart, dafs, wenn man β eine Wurzel der Gleichung

$$z^3 - 3z^2 - 4z - 1 = 0$$

nennt, z. B. diejenige, welche zwischen 4 und 5 liegt, die drei Wurzeln der gegebenen Gleichung bestimmt werden durch:

$$x = 1 + \frac{1}{1 + \frac{1}{\beta}} = \frac{2\beta + 1}{1 + \beta}$$

$$x_1 = \frac{1}{2 + \frac{1}{\beta}} = \frac{\beta}{2\beta + 1}$$

$$x_2 = -1 - \frac{1}{\beta} = -\frac{1 + \beta}{\beta},$$

oder, wenn man den ersten Wert von x mit α bezeichnet, so werden die beiden andern:

$$x_1 = \frac{1}{1 + \frac{1}{\alpha - 1}} = \frac{\alpha - 1}{\alpha}$$

$$x_2 = -\frac{1}{\alpha - 1}.$$

Diese Eigenschaften könnte man leicht mittelst der Formeln für die Sinus bestätigen, da ja

$$x = 2 \cos \frac{1}{7}\pi, \quad x_1 = 2 \cos \frac{3}{7}\pi, \quad x_2 = 2 \cos \frac{5}{7}\pi = -2 \cos \frac{2}{7}\pi$$

ist. Wir bemerken übrigens, dafs die in Rede stehende Gleichung ihren Ursprung aus der Gleichung $r^7 - 1 = 0$ herleitet, wenn man darin $r^2 + rx + 1 = 0$ setzt; sie würde auch dazu dienen einem Kreise ein reguläres Polygon von 7 und von 14 Seiten einzubeschreiben. Denn die Seite des regulären Siebenecks ist gleich

$$2 \sin \frac{1}{7}\pi = \sqrt{4 - x^2} = \frac{2}{\sqrt{7}}(x + 2)\left(x - \frac{3}{2}\right),$$

und die des Polygons von 14 Seiten ist gleich $2 \cos \frac{3}{7}\pi = x_1$.

Alle Gleichungen, welche sich auf die Teilung des Kreises beziehen, sind so beschaffen, dafs eine ihrer Wurzeln genügt, um alle andern rational zu bestimmen. Es giebt jedoch noch unendlich viele andere, welche dieselbe Erleichterung darbieten, und unter allen diesen Gleichungen mufs man besonders diejenigen hervorheben, bei denen die Kettenbruchentwicklung einer Wurzel ausreicht, um die Entwicklung aller andern Wurzeln zu geben.

106.

Beispiel 2.

Die Gleichung

$$x^4 - x^3 - 3x^2 + 2x + 1 = 0$$

würde die Wurzeln haben:

$$x = 2\cos\frac{\pi}{9}, \quad x = -2\cos\frac{2\pi}{9}, \quad x = 2\cos\frac{3\pi}{9}, \quad x = -2\cos\frac{4\pi}{9}.$$

Schliefst man aber die Wurzel $2\cos\frac{3\pi}{9}$, welche sich auf 1 reduciert, aus, so erhält man die Gleichung:

$$x^3 - 3x - 1 = 0,$$

deren Wurzeln sind:

$$x = 2\cos\frac{\pi}{9}, \quad x = -2\cos\frac{2\pi}{9}, \quad x = -2\cos\frac{4\pi}{9}.$$

Folgendes ist die Entwicklung der kleinsten Wurzel $-2\cos\frac{4\pi}{9}$:

$x^3 - 3x - 1 = 0$	-0	$-1:0$
$-z^3 + 3z^2 - 1 = 0$	2	$-0:1$
$3z^3 - 3z - 1 = 0$	1	$-1:2$
$-z^3 + 6z^2 + 9z + 3 = 0$	7	$-1:3$
$17z^3 - 54z^2 - 15z - 1 = 0$	3	$-8:23$
$-73z^3 + 120z^2 + 99z + 17 = 0$	2	$-25:72$
$111z^3 - 297z^2 - 318z - 73 = 0$	3	$-58:167$
$-703z^3 + 897z^2 + 702z + 111 = 0$	1	$-199:573$
$1007z^3 + 387z^2 - 1212z - 703 = 0$	1	$-257:740$
$-521z^3 + 2583z^2 + 3408z + 1007 = 0$	6	$-456:1313$
$1907z^3 - 21864z^2 - 6790z - 521 = 0$	11	$-2993:8618$
u. s. w.	u. s. w.	u. s. w.

Die letzte transformierte Gleichung hat zur Wurzel annähernd:

$$\frac{1313}{4309} + \frac{21864}{1907} = 11\,\frac{6325974}{8217263},$$

und die Entwicklung dieses Bruches giebt hinter 11 die Quotienten:

$$1, \quad 3, \quad 2, \quad 1, \quad 9, \quad 1, \quad 2, \quad 5, \quad \ldots,$$

mittelst deren die Berechnung der Näherungsbrüche noch so lange fortgesetzt werden kann, als die Nenner nicht gröfser sind als $(8618)^2$.

Entwicklung der Wurzel $x = 2\cos\frac{\pi}{9}$.

$x^3 - 3x - 1 = 0$	1	1 : 0
$-3z^3 + 3z + 1 = 0$	1	1 : 1
$z^3 - 6z^2 - 9z - 3 = 0$	7	2 : 1
$-17z^3 + 54z^2 + 15z + 1 = 0$	3	15 : 8
Die andern transformierten Gleichungen sind dieselben wie in der Entwicklung der ersten Wurzel.	2	47 : 25
	3	109 : 58
	1	374 : 199
	1	483 : 257
	6	857 : 456
	11	5625 : 2993.

Entwicklung der Wurzel $x = -2\cos\frac{2\pi}{9}$.

$x^3 - 3x - 1 = 0$	− 1	− 1 : 0
$z^3 - 3z - 1 = 0$	1	− 1 : 1
$-3z^3 + 3z + 1 = 0$	1	− 2 : 1
$z^3 - 6z^2 - 9z - 3 = 0$	7	− 3 : 2
Die andern transformierten Gleichungen wie bei der vorhergehenden Wurzel.	3	− 23 : 15
	2	− 72 : 47
	3	− 167 : 109
	1	− 573 : 374
	1	− 740 : 483
	6	− 1313 : 857
	11	− 8618 : 5625.

Diese Beziehungen zwischen den Wurzeln können leicht durch die bekannten Formeln für die Sinus bestätigt werden.

107.

Wir haben schon bemerkt (No. 101), dafs, wenn die gegebene Gleichung ist:

$$ax^n + bx^{n-1} + cx^{n-2} + \cdots + k = 0,$$

und eine ihrer transformierten Gleichungen, welche dem Näherungsbruche $\frac{p}{q}$ entspricht, bezeichnet wird durch:

$$Az^n + Bz^{n-1} + Cz^{n-2} + \cdots + K = 0,$$

alsdann die Gleichung gilt:

$$A = ap^n + bp^{n-1}q + cp^{n-2}q^2 + \cdots + kq^n.$$

Soll demnach die unbestimmte Gleichung

$$at^n + bt^{n-1}u + ct^{n-2}u^2 + \cdots + ku^n = A$$

aufgelöst werden und findet sich die Zahl A als Koefficient des ersten Gliedes in einer der aufeinanderfolgenden transformierten Gleichungen, welche durch Entwicklung von x in einen Kettenbruch gegeben werden, so wird der entsprechende Bruch $\frac{p}{q}$ ein Wert von $\frac{t}{u}$ sein und eine Lösung der gegebenen Gleichung ergeben. Man wird daher auf diese Weise ebenso viele von diesen besonderen Lösungen erhalten, als sich die Zahl A unter den betreffenden Koefficienten vorfindet. Es ist jedoch noch aufserdem erforderlich, dafs das Zeichen dieses Koefficienten, so wie es durch die Rechnung geliefert wird, mit dem Zeichen von A auf der rechten Seite der vorgelegten Gleichung übereinstimmt. Diese Bedingung wird man stets erreichen, wenn n ungerade ist; sie kann indessen nicht erfüllt werden, wenn n gerade ist.

Um von der gegebenen Gleichung zu der transformierten Gleichung in z überzugehen, kann man direkt setzen:

$$x = \frac{pz + p^0}{qz + q^0}.$$

Umgekehrt kann man, um von der transformierten Gleichung auf die gegebene zurückzukommen,

$$z = \frac{q^0 x - p^0}{p - qx}$$

setzen. Dies giebt:

$$\pm a = A(-q^0)^n + B(-q^0)^{n-1}q + C(-q^0)^{n-2}q^2 + \cdots + Kq^n,$$

so dafs man, wenn die Gleichung

$$a = Ay^n + By^{n-1}u + Cy^{n-2}u^2 + \cdots + Ku^n$$

aufgelöst werden sollte, derselben genügen könnte, indem man

$$\frac{y}{u} = \frac{-q^0}{q}$$

nimmt. Das Verhältnis, dafs wir hier zwischen der gegebenen Gleichung und jeder ihrer transformierten Gleichungen feststellen, gilt in gleicher Weise zwischen irgend zwei transformierten Gleichungen, vorausgesetzt, dafs die Näherungsbrüche nach den zwischenliegenden Quotienten berechnet werden.

So kann man in dem ersten Beispiele direkt die zweite transformierte Gleichung

$$x^3 - 3x^3 - 4x - 1 = 0$$

mit der neunten

$$-47879z^3 + 250158z^2 + 50699z + 2521 = 0$$

vergleichen; jedoch mufs man dazu die Näherungsbrüche einer Wurzel der Gleichung $x^3 - 3x^2 - 4x - 1 = 0$ berechnen, und dies geschieht mit Hülfe der gefundenen Quotienten 4, 20, 2, 3, 1, 6, 10. Folgendes ist die Rechnung:

Quotienten: $\quad 4, \; 20, \; 2, \; 3, \; 1, \; 6, \; 10$

Näherungsbrüche: $\frac{1}{0}, \; \frac{4}{1}, \; \frac{81}{20}, \; \frac{166}{41}, \; \frac{579}{143}, \; \frac{745}{184}, \; \frac{5049}{1247}, \; \frac{51235}{12654}.$

Man erhält also:

$$x = \frac{51235z + 5049}{12654z + 1247}, \quad \text{oder} \quad z = \frac{-1247x + 5049}{12654x - 51235}.$$

Zugleich sieht man, dafs, wenn die Gleichung

$$47879t^3 + 250158t^2u - 50699tu^2 + 2521u^3 = 1$$

aufzulösen wäre, man derselben genügen könnte, indem man $t = 1247$ und $u = 12654$ setzt.

Eine solche Beziehung zwischen so grofsen Zahlen erscheint bemerkenswert; indessen erkennt man nach kurzer Überlegung, dafs alle transformierten Gleichungen, welche bei der Entwicklung einer und derselben Wurzel vorkommen, die nämliche Eigenschaft besitzen, mit andern Worten, dafs, wenn irgend eine dieser transformierten Gleichungen durch

$$Az^3 + Bz^2 + Cz + D = 0$$

dargestellt wird, wobei die Zahlen A, B, C, D zu beliebiger Gröfse anwachsen können, man immer der Gleichung

$$At^3 + Bt^2u + Ctu^2 + Du^3 = \pm 1$$

genügen kann, indem man $t = -q^0$ und $u = q$ setzt, wobei $\frac{p}{q}$ der dem vollständigen Quotient z entsprechende Näherungsbruch ist.

Beachtet man ferner, dafs die gegebene Gleichung

$$x^3 - x^2 - 2x + 1 = 0$$

und ihre drei ersten transformierten Gleichungen in ihrem ersten Gliede die Einheit zum Koefficienten haben, und dafs jede von diesen vier Gleichungen als die ursprüngliche Gleichung, welche durch Entwicklung ihrer Wurzel alle andern transformierten Gleichungen liefert, angesehen werden kann, so folgt daraus, dafs es mindestens vier Arten giebt, die Gröfse

$$At^3 + Bt^2u + Ctu^2 + Du^3$$

in 1 zu verwandeln. Z. B. kann man, wenn man sich die Gleichung

$$47879\,t^3 + 250158\,t^2u - 50699\,tu^2 + 2521\,u^3 = 1$$

vorlegt, derselben auf folgende vier Arten genügen:

$$t = 6296 \qquad u = 63889$$
$$t = 5049 \qquad u = 51235$$
$$t = 1247 \qquad u = 12654$$
$$t = 61 \qquad u = 619.$$

108.

Man kann jedoch auch noch andere Lösungen mittelst der Entwicklung der beiden andern Wurzeln der nämlichen Gleichung finden. Da man nämlich, wenn man von der Gleichung

$$47879\,z^3 + 250158\,z^2 - 50699\,z + 2521 = 0$$

ausgeht und darin

$$z = \frac{6296\,x - 11345}{63889\,x - 115124}$$

setzt, die transformierte Gleichung

$$x^3 - x^2 - 2x + 1 = 0$$

erhält, so kann man annehmen, dafs man zu diesem Resultat durch die Kettenbruchentwicklung einer zwischen 0 und 1 gelegenen Wurzel der Gleichung in z gelangt sei. Die Rechnung, welche die Umkehrung jener im Beispiel 1 wäre, ist folgende:

$0 = 47879\,z^3 + 250158\,z^2 - 50699\,z + 2521$	0	1 : 0
$0 = 2521\,y^3 - 50699\,y^2 + 250158\,y + 47879$	10	0 : 1
$0 = 559\,y^3 - 7522\,y^2 + 24931\,y + 2521$	6	1 : 10
$0 = 2059\,y^3 - 4961\,y^2 + 2540\,y + 559$	1	6 : 61
$0 = 197\,y^3 - 1205\,y^2 + 1216\,y + 2059$	3	7 : 71
$0 = 181\,y^3 - 695\,y^2 + 568\,y + 197$	2	27 : 274
$0 = y^3 - 40\,y^2 + 391\,y + 181$	20	61 : 619
$0 = y^3 - 9\,y^2 + 20\,y + 1$	4	1247 : 12654
$0 = y^3 - 4\,y^2 + 3\,y + 1$	1	5049 : 51235
$*0 = y^3 - 2\,y^2 - y + 1$	1*	6296 : 63889
$0 = - Z^3 - 2Z^2 + Z + 1$		11345 : 115124

Bei dieser transformierten Gleichung angelangt, würde man haben:

$$z = \frac{11345 Z + 6396}{115124 Z + 63889}.$$

Setzt man also $-\frac{1}{x}$ an Stelle von Z, so sieht man, dafs die Substitution des Wertes

$$z = \frac{6296 x - 11345}{63889 x - 115124}$$

in der That die transformierte Gleichung liefert:

$$x^3 - x^2 - 2x + 1 = 0.$$

Die vorstehende Entwicklung, welche bis zur vorletzten transformierten Gleichung genau ist, hört indessen bei der letzten auf es zu sein; aus diesem Grunde haben wir die letzten Resultate, da dieselben erst noch bestätigt werden müssen, durch einen Strich abgetrennt.

Die vorletzte transformierte Gleichung

$$0 = y^3 - 2y^2 - y + 1$$

hat zwei positive Wurzeln, von denen die eine zwischen 0 und 1, die andere zwischen 2 und 3 liegt. Macht man zunächst von der letzteren Gebrauch, so mufs man 2 als angenäherten Wert der Wurzel nehmen, an Stelle von 1*, welcher in dem vorhergehenden Schema enthalten ist. Alsdann setzt sich die Rechnung folgendermafsen fort:

		5049 : 51235
$*0 = y^3 - 2y^2 - y + 1$	2	6296 : 63889
$0 = -y^3 + 3y^2 + 4y + 1$	4	17641 : 179013
$0 = y^3 - 20y^2 - 9y - 1$	20	76860 : 779941
$0 = -181y^3 + 391y^2 + 40y + 1$	2	1554841 : 15777833
Folgen dieselben transformierten Gleichungen und dieselben Quotienten wie im Beispiel 1.	u. s. w.	u. s. w.

Da man hier zwei neue transformierte Gleichungen findet, deren erstes Glied den Koefficienten 1 hat, so folgt daraus, dafs die unbestimmte Gleichung

$$47879 t^3 + 250158 t^2 u - 50699 t u^2 + 2521 u^3 = \pm 1$$

zwei neue Lösungen besitzt, nämlich:

$t = 17641, \quad u = 179013,$ rechte Seite -1

$t = 76860 \quad u = 779941,$ rechte Seite $+1$.



Macht man sodann von der zwischen 0 und 1 liegenden Wurzel Gebrauch, so mufs man überdies den Quotienten berichtigen, welcher vor der vorhergehenden transformierten Gleichung

$$0 = y^3 - 4y^2 + 3y + 1$$

steht, und erhält so die folgenden Resultate, welche die Entwicklung eines zweiten Wertes von z darstellen:

		1247 : 12654
$0 = y^3 - 4y^2 + 3y + 1$	2	5049 : 51235
$0 = -y^3 - y^2 + 2y + 1$	1	11345 : 115124
$0 = y^3 - 3y^2 - 4y - 1$	4	16394 : 166359
$0 = -y^3 + 20y^2 + 9y + 1$	20	76921 : 780560
$0 = 181y^3 - 391y^2 - 40y - 1$	2	1554814 : 15777559
Das Übrige wie oben.	3	u. s. w.
	1	
	u. s. w.	

Man erhält daher noch drei neue Werte, welche der unbestimmten Gleichung genügen, nämlich:

$t = 11345$, $u = 115124$, rechte Seite -1

$t = 16394$, $u = 166359$, rechte Seite $+1$

$t = 76921$, $u = 780560$, rechte Seite -1.

109.

Um über diese Theorie noch weiteres Licht zu verbreiten, betrachten wir allgemein eine gegebene Gleichung $X = 0$ und setzen voraus, dafs man bei der Kettenbruchentwicklung einer ihrer Wurzeln zu irgend einer transformierten Gleichung $Z = 0$ gelange. Es sei $\alpha, \beta, \ldots \mu, \ldots$ die Reihe der gefundenen Quotienten und $\frac{p}{q}$ der Näherungsbruch, welcher sowohl dem ganzzahligen Quotienten μ wie dem durch die Gleichung $Z = 0$ gegebenen vollständigen Quotienten z entspricht. Folgendes stellt das Schema der Entwicklung dar:

$X = 0$	α	$1:0$
.	β	$\alpha:1$
.	γ	:
.	δ	:
.	.	:
.	.	:
.	μ^0	$p^0:q^0$
$Z = 0$	μ	$p:q$
$Z' = 0$	μ'	$p':q'$
.	.	.
.	.	.

Dieses vorausgeschickt, ergiebt sich die transformierte Gleichung $Z = 0$ unmittelbar aus der gegebenen, wenn man an Stelle von x den Wert

$$x = \frac{pz + p^0}{qz + q^0}$$

setzt. Umgekehrt würde die gegebene Gleichung $X = 0$ aus irgend einer der transformierten Gleichungen $Z = 0$ entstehen, wenn man in dieser für z den Wert

$$z = \frac{q^0 x - p^0}{p - qx}$$

setzt. Dieselbe Beziehung läſst sich nachweisen zwischen irgend zwei transformierten Gleichungen, wofern nur die Näherungsbrüche mittelst der zwischenliegenden Quotienten berechnet werden, indem man von demjenigen ausgeht, welcher der ersteren transformierten Gleichung entspricht und ein angenäherter Wert ihrer Wurzel ist.

Es ist leicht zu sehen, daſs die Formel

$$x = \frac{pz + p^0}{qz + q^0}$$

implicitè alle Wurzeln der gegebenen Gleichung in sich faſst; denn man kann sich denken, daſs man der Reihe nach für z alle Wurzeln der Gleichung $Z = 0$ einsetzt, woraus sich ebenso viele verschiedene Werte von x ergeben.

Umgekehrt enthält der Wert

$$z = \frac{q^0 x - p^0}{p - qx}$$

alle Wurzeln der transformierten Gleichung $Z = 0$. Eine dieser Wurzeln, welche positiv und gröſser als die Einheit ist, wird

gegeben durch die Fortsetzung der Kettenbruchentwicklung, so dafs man hat:

$$z = \mu + \frac{1}{\mu'} + \frac{1}{\mu''} + \text{in inf.}$$

Dieselbe mufs als der in einen Kettenbruch entwickelten Wurzel x entsprechend betrachtet werden. Die andern Wurzeln der transformierten Gleichung (wenigstens wenn die Entwicklung regulär geworden ist und die transformierte Gleichung nicht zugleich zwei Wurzeln hat, die positiv und gröfser als 1 sind) sind sämtlich negativ und kleiner als 1. Bezeichnet man nämlich durch x_1 diejenige von den übrigen Wurzeln der gegebenen Gleichung, welche einer andern, in analoger Weise mit z_1 bezeichneten, Wurzel der transformierten Gleichung entspricht, so hat man:

$$z_1 = \frac{q^0 x_1 - p^0}{p - q x_1} = -\frac{p^0}{p} + \frac{(p q^0 - p^0 q) x_1}{p(p - q x_1)}.$$

Nun ist aber $pq^0 - p^0 q = \pm 1$; ferner wächst p und somit $p - qx_1$, da $\frac{p}{q}$ kein Näherungsbruch von x_1 ist. Es ist daher klar, dafs der Wert von z_1 sich um so mehr $\frac{-p^0}{p}$ nähert, je gröfser p wird. Dieses Ergebnis findet in gleicher Weise für jede andere Wurzel der transformierten Gleichung aufser für z statt; daraus erkennt man, dafs alle diese Wurzeln unter einander gleich zu werden streben, und dafs sie sich dem gemeinsamen Werte $\frac{-p^0}{p}$, welcher eine negative Gröfse und kleiner als 1 ist, nähern.

110.

Andrerseits weifs man (No. 11), dafs die Gröfse $\frac{p^0}{p}$ gleich dem Kettenbruche ist:

$$\frac{1}{\mu^0} + \frac{1}{\mu^{00}} + \frac{1}{\mu^{000}} + \cdots + \frac{1}{\alpha},$$

welcher aus den Quotienten, welche μ in umgekehrter Reihenfolge vorangehen, bis zum ersten α einschliefslich, gebildet ist. Während also eine Wurzel z der transformierten Gleichung $Z = 0$ bei ihrer Entwicklung die Quotienten μ, μ', μ'', ... giebt, ergeben alle andern Wurzeln derselben transformierten Gleichung bei ihrer Entwicklung die vorhergehenden Quotienten μ^0, μ^{00}, μ^{000}, ... in umgekehrter Reihen-

folge. Diese Wurzeln sind daher in der That um so näher einander gleich, je gröſser das Intervall zwischen der gegebenen und der betreffenden transformierten Gleichung ist. Aber wie angenähert richtig auch diese Gleichheit sein möge, sie wird niemals in aller Strenge stattfinden, und man kann stets die verschiedenen Werte von z_1, welche den analogen Werten von x_1 entsprechen, für sich entwickeln.

Denn bildet man wieder den Bruch $\frac{p^0}{p}$ mittelst der ihn erzeugenden Quotienten, also:

$$\begin{array}{ccccc} \mu^0, & \mu^{00}, & \mu^{000}, & \ldots\ \beta, & \alpha \\ \frac{0}{1}, & \frac{1}{\mu^0} & . & \ldots\ . \ \frac{q^0}{q}, & \frac{p^0}{p}, \end{array}$$

und setzt man darauf $\alpha - x_1$ an die Stelle von α, so geht der Kettenbruch offenbar über in $\frac{p^0 - q^0 x_1}{p - q x_1}$, und man erhält demnach:

$$-z_1 = \frac{p^0 - q^0 x_1}{p - q x_1}.$$

Mithin ist der genaue, in einen Kettenbruch entwickelte Wert von $-z_1$ der folgende:

$$-z_1 = \frac{1}{\mu^0} + \frac{1}{\mu^{00}} + \cdots + \frac{1}{\alpha - x_1}.$$

Man hat also nur noch für x_1 seinen Wert, ausgedrückt ebenfalls durch einen Kettenbruch, einzusetzen. Dazu müssen wir verschiedene Fälle untersuchen.

1) Ist x_1 negativ und fängt die Entwicklung seines Wertes folgendermaſsen an:

$$-x_1 = \alpha_1 + \frac{1}{\beta_1} + \frac{1}{\gamma_1} + \cdots,$$

so ist klar, daſs die Verknüpfung der beiden Kettenbrüche ohne Schwierigkeiten ausgeführt werden kann und ergiebt:

$$-z_1 = \frac{1}{\mu^0} + \frac{1}{\mu^{00}} + \cdots + \frac{1}{\beta} + \frac{1}{\alpha + \alpha_1} + \frac{1}{\beta_1} + \cdots$$

2) Ist der Wert von x_1 positiv und kleiner als α, so setze man:

$$x_1 = \alpha_1 + \frac{1}{y}.$$

Dies giebt:

$$\alpha - x_1 = \alpha - \alpha_1 - 1 + \frac{1}{1} + \frac{1}{-1+y}.$$

Im Falle, daſs $\alpha - \alpha_1 = 1$ ist, muſs man auf den α vorangehenden Quotienten zurückgehen und erhält dann:

$$\beta + \frac{1}{\alpha - x_1} = \beta + 1 + \frac{1}{-1+y}.$$

3) Ist der Wert von x_1 positiv und gröſser als α, so muſs man ebenfalls auf den Quotienten β zurückgehen und erhält:

$$\beta + \frac{1}{\alpha - x_1} = \beta + \frac{1}{\alpha - \alpha_1 - \frac{1}{y}}.$$

Ist zuerst $\alpha = \alpha_1$, so reduciert sich dieser Wert auf $\beta - y$ und man kann hinsichtlich des Wertes $\beta - y$ ebenso verfahren, wie es bei $\alpha - x$ geschehen ist.

Ist ferner $\alpha - \alpha_1 = -m$, so erhält man:

$$\beta + \frac{1}{\alpha - x_1} = \beta - \frac{1}{m + \frac{1}{y}} = \beta - 1 + \frac{1}{1} + \frac{1}{m - 1 + \frac{1}{y}}.$$

Daraus sieht man, daſs in allen Fällen die Substitution des Wertes von x_1 in dem Kettenbruche für z_1 ausgeführt werden kann, ohne daſs eine andere Änderung veranlaſst würde, als in einigen der letzten Glieder der Reihe μ^0, μ^{00}, ... β, α oder in einigen der ersten Glieder der Reihe α_1, β_1, γ_1, ..., welche aus der Entwicklung von x_1 herstammt. Übrigens wird die unendliche Reihe α_1, β_1, γ_1, ... (abgesehen vielleicht von einigen der ersten Glieder) gleichfalls in der Entwicklung von z_1 vorkommen. Mithin giebt eine beliebige Wurzel der transformierten Gleichung in ihrer Entwicklung stets dieselben Quotienten, wie die entsprechende Wurzel der gegebenen Gleichung, abgesehen von den ersten Gliedern, welche verschieden sind einmal wegen des der transformierten eigentümlichen Teiles μ^0, μ^{00}, ..., sodann wegen der Verknüpfung zweier Kettenbrüche, wodurch eine Änderung in den ersten Gliedern veranlaſst werden kann.

111.

Um diese Ergebnisse recht deutlich hervortreten zu lassen, nehmen wir das Beispiel 1 wieder auf, in welchem die gegebene Gleichung die folgende ist:

$$x^3 - x^2 - 2x + 1 = 0,$$

und betrachten eine ihrer transformierten Gleichungen, z. B.

$$-197z^3 + 568z^2 + 695z + 181 = 0.$$

Diejenige Wurzel, welche positiv und größer als 1 ist, wird durch die aus der Fortsetzung der Entwicklung entstehenden Quotienten 3, 1, 6, 10, 5, 2, 2, 1, 2, 2, 1, 18, 1, 1, 3, ... gegeben, so daß man für diese erste Wurzel erhält:

$$z = 3 + \frac{1}{1+}\frac{1}{6+}\frac{1}{10+}\frac{1}{5+}\cdots$$

Um die beiden andern Wurzeln derselben Gleichung zu erhalten, muß man, dem Gesagten entsprechend,

$$-z_1 = \frac{1}{2+}\frac{1}{20+}\frac{1}{4+}\frac{1}{1+}\frac{1}{1-x_1}$$

nehmen und für x_1 nach einander die beiden andern Wurzeln der gegebenen Gleichung einsetzen. Da die Substitution der negativen Wurzel am leichtesten ist, so nehmen wir zuerst den entwickelten Wert dieser Wurzel, welcher

$$-x_1 = 1 + \frac{1}{4+}\frac{1}{20+}\frac{1}{2+}\frac{1}{3+}\cdots$$

lautet, und erhalten so:

$$-z_1 = \frac{1}{2+}\frac{1}{20+}\frac{1}{4+}\frac{1}{1+}\frac{1}{2+}\frac{1}{4+}\frac{1}{20+}\frac{1}{2+}\frac{1}{3+}\frac{1}{1+}\frac{1}{6+}\cdots$$

Nimmt man sodann die dritte positive Wurzel:

$$x_2 = 0 + \frac{1}{2+}\frac{1}{4+}\frac{1}{20+}\cdots,$$

und setzt man zur Abkürzung:

$$x_2 = \frac{1}{2+}\frac{1}{y},$$

so erhält man die dritte Wurzel der transformierten Gleichung:

$$-z_2 = \frac{1}{2+}\frac{1}{20+}\frac{1}{4+}\frac{1}{1+}\frac{1}{1-}\frac{1}{2+}\frac{1}{y}.$$

Um in diesem Werte die Irregulärität wegzuschaffen, mufs man die letzten Glieder des Kettenbruches folgendermafsen abändern:

$$\frac{1}{1+\frac{1}{1-\frac{1}{2+\frac{1}{y}}}} = \frac{y+1}{3y+2} = \frac{1}{2+\frac{y}{y+1}} = \frac{1}{2+\frac{1}{1+\frac{1}{y}}}.$$

Man hat daher ohne ein negatives Glied:

$$-z_2 = \frac{1}{2+\frac{1}{20+\frac{1}{4+\frac{1}{2+\frac{1}{1+\frac{1}{4+\frac{1}{20+\frac{1}{2+\frac{1}{3+\cdots}}}}}}}}}$$

Die nachfolgenden Quotienten sind wie bei der ersten Wurzel 1, 6, 10, 5, 2, 2, 1, 2, 2, 1, 18, 1, 1, 3...

Wenn man ferner diese Theorie auf die Gleichungen zweiten Grades anwendet und diejenige transformierte Gleichung betrachtet, welche den Wert des vollständigen Quotienten in einer entfernten Periode giebt, so findet man, dafs die zweite Wurzel der transformierten Gleichung ausgedrückt wird durch die vorhergehenden, in umgekehrter Reihenfolge genommenen Quotienten. Daraus geht hervor, dafs die Periode, welche bei der Entwicklung dieser zweiten Wurzel stattfindet, dieselbe ist, wie die der ersten, aber in umgekehrter Reihenfolge genommen. Dieses Resultat stimmt vollkommen überein mit demjenigen, welches wir bereits (§ 10) für die Gleichungen zweiten Grades gefunden haben.

112.

Obwohl im Vorhergehenden angenommen wurde, dafs die Koefficienten der gegebenen Gleichung ganze Zahlen seien, ist doch diese Bedingung nicht absolut erforderlich, und man kann, wenn es nöthig ist, die Wurzel jeder gegebenen Gleichung, mag letztere algebraisch oder auch transcendent sein, in einen Kettenbruch verwandeln. Dazu mufs man auf irgend eine Weise einen angenäherten Wert für die in Rede stehende Wurzel suchen und sodann diesen Wert in einen Kettenbruch entwickeln, indem man darauf achtet, dafs diese Entwicklung und die Berechnung der Näherungsbrüche an der Stelle abgebrochen werde, wo die Genauigkeit voraussichtlich aufhören mufs. Ist der Bruch $\frac{p}{q}$, bei welchem man abbricht, ein Näherungsbruch, so mufs man sich

daran erinnern, dafs der Unterschied zwischen diesem Bruche und x kleiner sein mufs als $\frac{1}{q^2}$. Da somit der Grad der Annäherung an den Wert von x bekannt ist, so kennt man auch die Grenze für q. Übrigens würde eine weitere Annäherung den Fehler, wenn es einen solchen giebt, wieder gut machen.

Wir nehmen also an, dafs man vermöge der ersten Annäherung die Quotienten und die Näherungsbrüche von x wie folgt gefunden habe:

Quotienten: $\alpha\,,\ \beta\,,\ \gamma\,,\ \ldots\ \mu^0$

Näherungsbrüche: $\frac{1}{0}\,,\ \frac{\alpha}{1}\,,\ \frac{\alpha\beta+1}{\beta}\,,\ \ldots\ \frac{p^0}{q^0}\,,\ \frac{p}{q}\,.$

Um die Entwicklung weiter fortzusetzen, nehme man die gegebene Gleichung $F(x) = 0$ und substituiere darin auf der linken Seite für x den Wert $\frac{p}{q} + \omega$. Dabei soll ω eine hinreichend kleine Korrektion sein, so dafs man die höheren Potenzen von ω im Vergleich zur ersten vernachlässigen kann. Setzt man dann

$$\frac{dF}{dx} = F',$$

so wird das Ergebnis der Substitution das folgende:

$$F\left(\frac{p}{q}\right) + \omega F'\left(\frac{p}{q}\right) = 0\,,$$

und hieraus folgt:

$$\omega = -\frac{F\left(\frac{p}{q}\right)}{F'\left(\frac{p}{q}\right)}\,.$$

Ist jetzt z der $\frac{p}{q}$ entsprechende vollständige Quotient, so hat man:

$$x = \frac{pz + p^0}{qz + q^0} = \frac{p}{q} + \omega\,,$$

und dies giebt, wenn man den Wert von ω einsetzt:

$$z = -\frac{q^0}{q} + (pq^0 - p^0q)\frac{F'\left(\frac{p}{q}\right)}{q^2F\left(\frac{p}{q}\right)}\,.$$

Ist die Gleichung algebraisch und hat man:

$$F(x) = ax^n + bx^{n-1} + cx^{n-2} + \cdots + k$$
$$F'(x) = nax^{n-1} + (n-1)bx^{n-2} + (n-2)cx^{n-3} + \cdots,$$

so ergiebt sich:

$$z = -\frac{q^0}{q} + \frac{pq^0 - p^0q}{q}\cdot\frac{nap^{n-1} + (n-1)bp^{n-2}q + (n-2)cp^{n-3}q^2 + \cdots}{ap^n + bp^{n-1}q + cp^{n-2}q^2 + \cdots + kq^n}\,,$$

und dies kommt auf die Formel in No. 102 zurück.

Im Allgemeinen ist zu bemerken, dafs der Wert von z durch Entwicklung verschiedene Quotienten μ, μ', μ'', ... liefert, die sich an die bereits gefundenen Quotienten anschliefsen und gestatten, die Berechnung der Näherungsbrüche fortzusetzen, bis sich der Fehler der ersten Annäherung auf sein Quadrat reduciert hat. Und wenn der Fall einträte, dafs der Wert von z nicht positiv und gröfser als die Einheit wäre, so wäre dies ein Beweis dafür, dafs einer oder mehrere der vorhergehenden Quotienten μ^0, μ^{00}, ... fehlerhaft sind und mit Hülfe des Wertes von z verbessert werden müfsten. Alsdann müfste man alles auf einen einzigen Bruch $\mu^0 + \frac{1}{z}$ reducieren, und wenn die Summe positiv und gröfser als die Einheit ist, so würde nur der letzte Quotient μ^0 zu ändern sein. Im entgegengesetzten Falle müfste man den Wert von z in

$$\mu^{00} + \frac{1}{\mu^0 + \frac{1}{z}} \quad \text{oder selbst in} \quad \mu^{000} + \frac{1}{\mu^{00} + \frac{1}{\mu^0 + \frac{1}{z}}}$$

substituieren, also indem man soweit zurückgeht, bis man zu einem Resultat gelangt, das positiv und gröfser als die Einheit ist. Wird dieser Wert in einen Kettenbruch entwickelt, so giebt er gleichzeitig die Quotienten, welche man an Stelle der fehlerhaften einsetzen mufs und einige der nächstfolgenden, je nach dem Grade der ersten Annäherung.

Offenbar kann man durch derartige, so oft, als nötig ist, wiederholte Rechnungen jede Wurzel einer gegebenen Gleichung, mag letztere beschaffen sein wie sie wolle, bis zu einer beliebigen Anzahl von Quotienten in einen Kettenbruch entwickeln.

113.

Was die Methode anbelangt, welche man befolgen mufs, um die erste Annäherung zu erhalten, so kann man als eine der einfachsten und zweckentsprechendsten die Methode von Daniel Bernoulli anführen, die sich auf die Theorie der rekurrenten Reihen gründet und von der Euler in seiner „Introductio in Analysin infinitorum“ Cap. XVII eine ausführliche Auseinandersetzung gegeben hat. Da jedoch diese Methode in den Anwendungen mancher Schwierigkeit unterliegt, so dürfte es nicht unnützlich sein, dieselbe hier mit einer Modifikation, die einen grofsen Teil dieser Schwierigkeiten zu beseitigen imstande ist, darzulegen.

Ist
$$x^m + ax^{m-1} + bx^{m-2} + cx^{m-3} + \cdots = 0$$
eine gegebene Gleichung, deren Wurzeln α, β, γ, δ, ... sind, und nimmt man für z eine beliebige Veränderliche, so hat man die identische Gleichung:
$$1 + az + bz^2 + cz^3 + \cdots = (1 - \alpha z)(1 - \beta z)(1 - \gamma z) \ldots$$
Hieraus ergiebt sich durch Differentiation folgende, ebenfalls identische Gleichung:
$$\frac{-a - 2bz - 3cz^2 - \cdots}{1 + az + bz^2 + cz^3 + \cdots} = \frac{\alpha}{1 - \alpha z} + \frac{\beta}{1 - \beta z} + \frac{\gamma}{1 - \gamma z} + \frac{\delta}{1 - \delta z} + \cdots$$
Ist
$$A + Bz + Cz^2 + Dz^3 + \cdots + Mz^{n-1} + Nz^n + \cdots$$
die Reihe, welche durch Entwicklung der linken Seite entsteht, so erhält man dem bekannten Gesetz der rekurrenten Reihe zufolge:
$$\begin{aligned} A &= -a \\ B &= -aA - 2b \\ C &= -aB - bA - 3c \\ D &= -aC - bB - cA - 4d \\ E &= -aD - bC - cB - dA - 5e \end{aligned}$$
u. s. w.

Es mufs demnach die also gefundene Reihe $A + Bz + Cz^2 + \cdots$ mit derjenigen identisch sein, welche aus der rechten Seite
$$\frac{\alpha}{1 - \alpha z} + \frac{\beta}{1 - \beta z} + \cdots$$
hervorgeht. Nun ist:
$$\frac{\alpha}{1 - \alpha z} = \alpha + \alpha^2 z + \alpha^3 z^2 + \cdots,$$
und ähnliche Resultate ergeben die anderen Partialbrüche. Vereinigt man also alle diese Resultate, so findet man:
$$\begin{aligned} A &= \alpha + \beta + \gamma + \delta + \varepsilon + \cdots \\ B &= \alpha^2 + \beta^2 + \gamma^2 + \delta^2 + \varepsilon^2 + \cdots \\ C &= \alpha^3 + \beta^3 + \gamma^3 + \delta^3 + \varepsilon^3 + \cdots \\ & \ldots\ldots\ldots\ldots\ldots, \end{aligned}$$
und allgemein:
$$N = \alpha^n + \beta^n + \gamma^n + \delta^n + \varepsilon^n + \cdots$$
Diese Formeln sind diejenigen, welche dazu dienen, die Potenzsummen der Wurzeln einer gegebenen Gleichung zu bestimmen; es ist jedoch ersichtlich, dafs sie auch auf die näherungsweise



Auflösung der Gleichungen anwendbar sind. Denn ist α die gröfste der Wurzeln, und ist der Exponent n hinreichend grofs, so ist ziemlich nahe $N = \alpha^n$; aus demselben Grunde ist $M = \alpha^{n-1}$, und daher die gesuchte Wurzel:

$$\alpha = \frac{N}{M}.$$

Um also die gröfste Wurzel der gegebenen Gleichung näherungsweise zu erhalten, mufs man nach dem Gesetz der rekurrenten Reihen die aufeinanderfolgenden Koefficienten $A, B, C, D, \ldots M, N, \ldots$ berechnen und den zuletzt gefundenen Koefficienten durch den vorletzten dividieren; das Resultat ist der Wert der verlangten Wurzel. Dieser Wert ist um so mehr angenähert, je weiter die Rechnung fortgesetzt ist und ein je gröfserer Unterschied zwischen den einzelnen Wurzeln stattfindet.

Durch eine Transformation kann man leicht bewirken, dafs eine beliebige Wurzel die gröfste der Wurzeln wird. Mithin kann dieses Verfahren dazu dienen, sämtliche Wurzeln ohne Unterschied zu finden. In einer grofsen Anzahl von Fällen wird die Annäherung auf diesem Wege schneller als auf irgend einem andern bekannten Wege erfolgen; zuweilen ist sie nur langsam und in einigen Fällen sind die erhaltenen Resultate ganz und gar falsch. Es ist jedoch leicht, diese Übelstände vorauszusehen und zu vermeiden, wenn man eine erste Vorstellung von der relativen Gröfse und der Beschaffenheit der Wurzeln hat.

114.

Wir wollen diese Methoden anwenden auf die Gleichung:

$$x^3 - 3x^2 + 1 = 0.$$

Um den angenäherten Wert der gröfsten Wurzel zu erhalten, mufs man den Bruch:

$$\frac{3 - 3z^2}{1 - 3z + z^3}$$

in eine Reihe entwickeln. Dies giebt:

$$3 + 9z + 24z^2 + 69z^3 + 198z^4 + 570z^5 + 1641z^6 + 4725z^7 \\ + 13605z^8 + 39174z^9 + \cdots$$

Bleibt man also bei dem zehnten Gliede stehen, so erhält man die gesuchte Wurzel:

$$x = \frac{39174}{13605}.$$

Entwickelt man jetzt diesen Wert in einen Kettenbruch, so erhält man die Quotienten 2, 1, 7, 3, 2, 3, 1, 2, 6. Um zu beurteilen, bis zu welchem Punkte sie genau richtig sein können, entwickle man ebenso den Bruch $\frac{13605}{4725}$, den man erhalten haben würde, wenn man beim neunten Gliede stehen geblieben wäre. Es ergeben sich aus diesem die Quotienten 2, 1, 7, 3, 2, 5. Darnach scheint es, als ob man die Quotienten 2, 1, 7, 3, 2, 3 als genau ansehen dürfe. Mittelst dieser berechnet man die Näherungsbrüche wie folgt:

Quotienten: 2, 1, 7, 3, 2, 3

Näherungsbrüche: $\frac{1}{0}, \frac{2}{1}, \frac{3}{1}, \frac{23}{8}, \frac{72}{25}, \frac{167}{58}, \frac{573}{199}$.

Um die Berechnung dieser Näherungsbrüche nach der Methode der No. 112 fortzusetzen, setzen wir:

$$\frac{p^0}{q^0} = \frac{167}{58}, \quad \frac{p}{q} = \frac{573}{199}.$$

Ferner sei stets z der vollständige Quotient, welcher diesem letzteren Bruche entspricht. Beachtet man dann, dafs $pq^0 - p^0q = +1$ ist, so hat man:

$$z = -\frac{q^0}{q} + \frac{1}{q}\,\frac{3p^2 - 6pq}{p^3 - 3p^2q + q^3} = \frac{260051}{139897}.$$

Da dieser Wert positiv und gröfser als die Einheit ist, so folgt daraus, dafs alle bisher angewendeten Quotienten genau sind. Um die nächstfolgenden zu erhalten, mufs man den Wert von z in einen Kettenbruch entwickeln. Dies giebt die neuen Quotienten 1, 1, 6, 11, 1, 1, 1, 3 . . ., so dafs sich die Berechnung der Entwicklung in folgender Weise fortsetzt:

Quotienten: 1, 1, 6, 11, 1

Näherungsbrüche: $\frac{167}{58}, \frac{573}{199}, \frac{740}{257}, \frac{1313}{456}, \frac{8618}{2993}, \frac{96111}{33379}, \frac{104729}{36372}, \ldots$

Bei diesem letzteren bleibt man stehen, da 36372 ebensoviel Ziffern hat, als das Quadrat von 199, und der folgende Bruch nicht mehr zur Zahl der Näherungsbrüche gehören könnte.

115.

Die soeben entwickelten Methoden beziehen sich nur auf die reellen Wurzeln der Gleichungen. Mit Bezug auf die **imaginären** Wurzeln dürfte es ebenfalls nützlich sein, einen beliebig angenäherten Ausdruck zu haben; denn die unbestimmte Analysis bietet Fälle dar, wo es erforderlich ist, den

reellen Teil dieser Wurzeln in einen Kettenbruch zu entwickeln. Wir benutzen die Gelegenheit, um **einige neue Gesichtspunkte über die näherungsweise Berechnung der imaginären** Wurzeln beizubringen, ein Gegenstand, der bisher von den Analysten ziemlich vernachlässigt worden ist.

Man weifs, dafs jede imaginäre Wurzel einer Gleichung dargestellt werden kann durch $\alpha + \beta\sqrt{-1}$, wo α und β reelle Gröfsen sind. Man weifs ferner, dafs sich die Gröfse α direkt durch eine Gleichung vom Grade $\frac{n(n-1)}{2}$, wo n der Grad der gegebenen Gleichung ist, bestimmen läfst. Hat man α gefunden, so ist es nicht schwer, β zu erhalten. Denn da die Gleichung durch

$$x^2 - 2\alpha x + \alpha^2 + \beta^2$$

teilbar sein mufs, so mufs man, wenn die Division ausgeführt wird und der Rest $Ax + B$ ist, die beiden Gleichungen $A = 0$ und $B = 0$ erhalten, aus denen man einen rationalen Wert von β^2 als Funktion von α herleiten kann. Es reduciert sich also alles darauf, den Wert von α mit Hülfe der Gleichung, von der er abhängt, und die sich durch Kombination der Gleichungen $A = 0$ und $B = 0$ ergiebt, zu finden. Sobald aber n gröfser ist als 4, wird der Grad dieser Gleichung viel zu hoch, als dafs sie in der Praxis von einigem Nutzen sein könnte. Man mufs demnach durchaus zu andern Mitteln greifen, um angenäherte Werte für α und β zu erhalten. Nun kann man aber immer, welches auch α und β sein mögen,

$$\alpha = r\cos\varphi, \quad \beta = r\sin\varphi$$

setzen. Dies giebt:

$$x = r(\cos\varphi + \sqrt{-1}\sin\varphi),$$

und allgemein:

$$x^m = r^m(\cos m\varphi + \sqrt{-1}\sin m\varphi).$$

Diese Formeln, deren Anwendung Euler gezeigt hat, dienen dazu, in gewissen Fällen die Untersuchung der imaginären Wurzeln bedeutend zu vereinfachen.

116.

Es sei zunächst die Gleichung

$$ax^m + bx + c = 0$$

gegeben, auf welche sich jede aus drei Gliedern bestehende Gleichung reducieren läfst. (Wir setzen nämlich nicht voraus, dafs m eine ganze Zahl sei.) Setzt man für x den Wert $r(\cos\varphi + \sqrt{-1}\sin\varphi)$, so

zerlegt sich die gegebene Gleichung in die beiden andern:

$$0 = ar^m \cos m\varphi + br \cos \varphi + c$$

$$0 = ar^m \sin m\varphi + br \sin \varphi.$$

Multipliciert man die erste mit $\sin m\varphi$, die zweite mit $-\cos m\varphi$ und addiert sodann die Produkte, so erhält man:

$$0 = c \sin m\varphi + br \sin (m-1)\varphi,$$

und daher:

$$r = -\frac{c}{b} \cdot \frac{\sin m\varphi}{\sin (m-1)\varphi}.$$

Substituiert man diesen Wert in die zweite der vorhergehenden Gleichungen, so erhält man zur Bestimmung von φ die Gleichung:

$$\frac{\sin^m (m\varphi)}{\sin \varphi \sin^{m-1} (m-1)\varphi} = \frac{c}{a} \cdot \left(\frac{-b}{c}\right)^m.$$

Nach einigen Versuchen erkennt man nun bald, zwischen welchen aufeinanderfolgenden Graden der Winkel φ liegt; sodann führt man nach der Regel vom falschen Satze die Bestimmung von φ mit jeder Genauigkeit, welche die Tafeln bieten, d. h. gewöhnlich mit sechs oder sieben Ziffern zu Ende. Ist φ bekannt, so ist es auch r. Mithin kennt man die imaginäre Wurzel $r(\cos \varphi + \sqrt{-1} \sin \varphi)$ für die meisten Anwendungen genau genug.

117.

Wir wollen als Beispiel die Gleichung nehmen:

$$x^4 - x + 1 = 0.$$

Setzt man $x = r(\cos \varphi + \sqrt{-1} \sin \varphi)$, so erhält man:

$$r = \frac{\sin 4\varphi}{\sin 3\varphi},$$

und die Gleichung zur Bestimmung von φ wird:

$$\frac{\sin^4 4\varphi}{\sin \varphi \cdot \sin^3 3\varphi} = 1.$$

Setzt man $\varphi = 30^0$, so reduciert sich die linke Seite auf $\frac{9}{8}$; somit ist der Fehler gleich $+\frac{1}{8}$. Setzt man $\varphi = 31^0$, so wird die linke Seite 0,921, und dies giebt den Fehler $-0{,}079$. Man findet daher nahezu

$$\varphi = 30^0 36'.$$

Ist also $\varphi = 30^0 36'$, so ist der Logarithmus der linken Seite gleich 9,999933, und somit der Fehler gleich -67 Einheiten der sechsten Decimalstelle. Macht man $\varphi = 30^0 35'$, so wird der logarithmische

Fehler $+ 1394$. Daraus erhält man den wahren Wert von φ, angenähert soweit, als es die sechsstelligen Tafeln gestatten:

$$\varphi = 30^0 35',954.$$

Sodann findet man:

$$\log r = 9{,}926739$$
$$\log \alpha = 9{,}861615$$
$$\log \beta = 9{,}633482,$$

und demnach endlich die gesuchte Wurzel:

$$x = 0{,}727136 + 0{,}430014 \sqrt{-1}.$$

118.

Wir betrachten jetzt die allgemeine Gleichung:

$$ax^n + bx^{n-1} + cx^{n-2} + \cdots + hx + k = 0.$$

Setzt man darin den Wert $x = r(\cos\varphi + \sqrt{-1}\sin\varphi)$ ein und macht zur Abkürzung:

$$P = ar^n \cos n\varphi + br^{n-1}\cos(n-1)\varphi + \cdots + hr\cos\varphi + k$$
$$Q = ar^n \sin n\varphi + br^{n-1}\sin(n-1)\varphi + \cdots + hr\sin\varphi,$$

so wird das Resultat der Substitution

$$P + Q\sqrt{-1} = 0$$

sein, so dafs man zur Bestimmung von r und φ die beiden Gleichungen erhält:

$$P = 0, \qquad Q = 0.$$

Da jedoch die wirkliche Auflösung dieser Gleichungen nur in einer geringen Anzahl von Fällen möglich ist, die sich kaum über den Cotesischen Satz hinauserstrecken, so müssen wir uns darauf beschränken, dieselben durch Annäherung aufzulösen.

Wir nehmen also an, dafs man nach einigen Versuchen Werte von φ und r gefunden habe, für welche P und Q sehr klein werden. Um noch näher kommende Werte zu erhalten, bezeichnen wir letztere durch $\varphi + d\varphi$, $r + dr$. Es müssen daher, wenn man an Stelle von r und φ die Werte $r + dr$ und $\varphi + d\varphi$ in die Funktionen P und Q einsetzt, diese beiden Funktionen gleich Null werden. Vernachlässigt man nun die Potenzen von dr und $d\varphi$, welche höher sind als die erste, so wird die Gröfse P allgemein durch die in Rede stehende Substitution übergehen in:

$$P + \frac{r\,dP}{dr}\,\frac{dr}{r} + \frac{dP}{d\varphi}\,d\varphi,$$

und hierin sind die Koefficienten:

$$r\frac{dP}{dr} = \quad nar^n \cos n\varphi + (n-1)br^{n-1}\cos(n-1)\varphi + \cdots + hr\cos\varphi$$

$$\frac{dP}{d\varphi} = -nar^n \sin n\varphi - (n-1)br^{n-1}\sin(n-1)\varphi - \cdots - hr\sin\varphi.$$

Da ebenso die Gröſse Q übergeht in:

$$Q + \frac{rdQ}{dr}\frac{dr}{r} + \frac{dQ}{d\varphi}d\varphi,$$

so hat man:

$$r\frac{dQ}{dr} = nar^n \sin n\varphi + (n-1)br^{n-1}\sin(n-1)\varphi + \cdots + hr\sin\varphi$$

$$\frac{dQ}{d\varphi} = nar^n \cos n\varphi + (n-1)br^{n-1}\cos(n-1)\varphi + \cdots + hr\cos\varphi.$$

Man braucht also nur zwei Hülfsgröſsen M und N zu nehmen, welche durch die Werte gegeben sind:

$$M = nar^n \cos n\varphi + (n-1)br^{n-1}\cos(n-1)\varphi + \cdots + hr\cos\varphi$$

$$N = nar^n \sin n\varphi + (n-1)br^{n-1}\sin(n-1)\varphi + \cdots + hr\sin\varphi;$$

dann erhält man zur Bestimmung von dr und $d\varphi$ die beiden Gleichungen:

$$P + M\frac{dr}{r} - Nd\varphi = 0$$

$$Q + N\frac{dr}{r} + Md\varphi = 0,$$

aus denen folgt:

$$-\frac{dr}{r} = \frac{PM + QN}{M^2 + N^2}$$

$$d\varphi = \frac{PN - QM}{M^2 + N^2}.$$

Man findet auf diese Weise die verbesserten Werte von r und φ, nämlich $r\left(1 + \frac{dr}{r}\right)$ und $\varphi + d\varphi$, wobei zu beachten ist, daſs der durch die Formel gegebene Wert von $d\varphi$ in Teilen des Halbmessers ausgedrückt ist, und daſs derselbe somit, wenn man ihn in Minuten oder Sekunden verwandeln will, mit der Zahl der Minuten oder Sekunden, welche der Radius enthält, multipliciert werden muſs. Schlieſslich kann man diese Formeln noch bequemer für die trigonometrische Rechnung machen, wenn man zwei Winkel λ und μ und zwei Zahlen F und G bestimmt nach den Gleichungen:

$$\operatorname{tang}\lambda = \frac{P}{Q}, \qquad F = \frac{P}{\sin\lambda} = \frac{Q}{\cos\lambda}$$

$$\operatorname{tang}\mu = \frac{M}{N}, \qquad G = \frac{M}{\sin\mu} = \frac{N}{\cos\mu}.$$

Daraus folgt dann:

$$\frac{dr}{r} = -\frac{F}{G}\cos(\lambda - \mu)$$

$$d\varphi = \frac{F}{G}\sin(\lambda - \mu).$$

Ferner beachte man, dafs sich die Gröfsen M und N leicht mit Hülfe derselben Glieder bilden lassen, welche zur Bildung der Werte P und Q dienen; denn während

$$P = A + B + C + D + \cdots$$

ist, wo die aufeinanderfolgenden Glieder A, B, ... bezüglich gleich $ar^n \cos n\varphi$, $br^{n-1}\cos(n-1)\varphi$, ... sind, wird der Wert von M ausgedrückt durch die Reihe:

$$nA + (n-1)B + (n-2)C + (n-3)D + \cdots$$

Ebenso wird der Wert von N mit Hülfe der Glieder, aus denen Q besteht, gebildet.

Nachdem man mittelst dieser Methode Werte gefunden hat, die den genauen Werten von r und φ noch näher kommen, kann man sich derselben wie einer ersten Annäherung bedienen, um neue noch mehr angenäherte Werte zu finden, und so weiter, bis man den Grad der Genauigkeit, welchen die Tafeln gestatten, vollkommen erreicht hat.

119.

Für die Anwendung der vorhergehenden Methode ist es unerläfslich, dafs man einen ersten angenäherten Wert der gesuchten imaginären Wurzel habe. Nun hat man aber bis heute keine allgemeine und praktisch anwendbare Methode, welche zu diesem Ziele führte. Daher werden die Analysten, hoffe ich, mit Vergnügen von derjenigen Kenntnis nehmen, die ich entwickeln werde. Die Anwendung derselben ist sehr einfach und sie scheint keiner Ausnahme zu unterliegen.

Die aufzulösende Gleichung stellen wir durch $F(x) = 0$ dar und nehmen an, dafs man $x = \alpha + \beta\sqrt{-1}$ setze, wo α und β beliebige reelle Gröfsen sind, die jedoch kleiner als die Grenze der reellen Wurzeln sein sollen, wo diese Grenze ebenso bestimmt wird, als ob die Gleichung deren hätte oder haben könnte.

Diesen hypothetischen Wert von x setzen wir in $F(x)$ ein und nehmen an, dafs sich dadurch $F(x) = P + Q\sqrt{-1}$ ergebe, wo P und Q reelle Gröfsen sind. Nachdem man noch $\frac{dF}{dx} = F'$ gesetzt,

substituiere man denselben Wert von x in F' und erhalte als Resultat:

$$F'(x) = M + N\sqrt{-1}.$$

Nimmt man eine reelle oder imaginäre unbestimmte Gröſse ω an, die sehr klein ist im Verhältnis zu $\sqrt{\alpha^2+\beta^2}$, so erhält man offenbar, wenn man

$$x = \alpha + \beta\sqrt{-1} + \omega$$

setzt und die höheren Potenzen von ω fortläſst:

$$F(\alpha + \beta\sqrt{-1} + \omega) = P + Q\sqrt{-1} + \omega\,(M + N\sqrt{-1}).$$

Da nun ω beliebig war, so kann man setzen:

$$\omega\,(M + N\sqrt{-1}) = -\,n\,(P + Q\sqrt{-1}),$$

wo n ein mehr oder minder kleiner positiver Bruch ist, dessen Gröſse später genauer festgestellt werden wird. Man hat somit:

$$\omega = -\,n\,\frac{PM + QN}{M^2 + N^2} - n\sqrt{-1}\,\frac{QM - PN}{M^2 + N^2},$$

und der verbesserte Wert $x = \alpha + \beta\sqrt{-1} + \omega$ giebt näherungsweise:

$$F(x) = (1 - n)\,(P + Q\sqrt{-1}).$$

Diese Gröſse ist im Verhältnis von $1 - n$ zu 1 kleiner als das Resultat, das wir unter der Annahme $x = \alpha + \beta\sqrt{-1}$ erhalten haben. Was n angeht, so kann es beliebig angenommen werden, jedoch so, daſs ω immer hinreichend klein im Verhältnis zu $\sqrt{\alpha^2+\beta^2}$ ist. Wenn P und Q bereits sehr klein im Verhältnis zu M und N wären, so könnte man $n = 1$ setzen. Alsdann würde der zweite Näherungswert $\alpha + \beta\sqrt{-1} + \omega$ mit demjenigen übereinstimmen, den man nach dem gewöhnlichen Verfahren (No. 118) findet, indem man annimmt, daſs $\alpha + \beta\sqrt{-1}$ ein erster Näherungswert von x ist. Sind dagegen P und Q nicht sehr klein im Verhältnis zu M und N, so nehme man für n nur eine Gröſse, die kleiner als 1 und klein genug ist, damit ω mehrere Mal in $\alpha + \beta\sqrt{-1}$ enthalten sei. Dies läſst groſsen Spielraum für die Wahl*).

---

*) Wenn man zwei imaginäre Gröſsen z. B. $\alpha + \beta\sqrt{-1}$, $\mu + \nu\sqrt{-1}$ hinsichtlich ihrer Gröſse mit einander vergleichen soll, so darf man diese Vergleichung nur so verstehen, daſs die reellen Gröſsen $\sqrt{\alpha^2+\beta^2}$, $\sqrt{\mu^2+\nu^2}$, welche man ihre Moduln nennen kann, verglichen werden. Es wird somit r der Modul jeder reducierten imaginären Gröſse von der Form $r\,(\cos\varphi + \sqrt{-1}\sin\varphi)$ sein.
Anm. d. Verf.

Wird der so verbesserte Wert von x wiederum durch $\alpha + \beta\sqrt{-1}$ dargestellt, und setzt man denselben in die Funktionen F und F' ein, so leitet man daraus in analoger Weise einen zweiten verbesserten Wert her, mittelst dessen das neue Resultat $P + Q\sqrt{-1}$ wiederum im Verhältnis von $1 - n$ zu 1 kleiner wird. So fährt man fort, bis sich $F(x)$ auf eine sehr kleine Gröfse reduciert, in welchem Falle man $n = 1$ setzen kann und die Annäherung sehr schnell erfolgt.

Man beachte wohl, dafs wegen der besonderen Beschaffenheit der imaginären Gröfsen die fortschreitende Verkleinerung von $F(x)$ keine Grenze haben kann. Denn selbst wenn $M = 0$ und $N = 0$ d. h. $\frac{dF}{dx} = 0$ wäre, so würde man, wenn man die Substitution von $x = \alpha + \beta\sqrt{-1}$ in den Funktionen $\frac{d^2F}{2\,dx^2}$, $\frac{d^3F}{2\cdot 3\,dx^3}$, u. s. w. ausführt, notwendigerweise zu einem Gliede kommen müssen, welches nicht verschwindet. Alsdann erhält man ein Resultat von der Form:

$$F(\alpha + \beta\sqrt{-1} + \omega) = P + Q\sqrt{-1} + \omega^k(T + V\sqrt{-1}),$$

wobei man

$$\omega^k(T + V\sqrt{-1}) = -n(P + Q\sqrt{-1})$$

setzen kann. Um hieraus den Wert von ω herzuleiten, bestimme man r und μ so, dafs

$$r(\cos\mu + \sqrt{-1}\sin\mu) = -n\frac{P + Q\sqrt{-1}}{T + V\sqrt{-1}}$$

ist. Man hat dann also:

$$\omega^k = r(\cos\mu + \sqrt{-1}\sin\mu),$$

und daher:

$$\omega = r^{\frac{1}{k}}\left(\cos\frac{\mu}{k} + \sqrt{-1}\sin\frac{\mu}{k}\right).$$

Setzt man also $x = \alpha + \beta\sqrt{-1} + \omega$, so hat man sehr nahe:

$$F(x) = (1 - n)(P + Q\sqrt{-1}).$$

Verkleinert man daher $F(x)$ fortgesetzt durch solche zweckmäfsig wiederholte Rechnungen, so wird man offenbar zu einem Werte von $F(x)$ gelangen, der so klein ist als man will, und alsdann wird der Wert von x bekannt sein.

Es ist somit auf eine ebenso einfache wie direkte Weise bewiesen, dafs ein Wert von x von der Form $\alpha + \beta\sqrt{-1}$ immer der gegebenen Gleichung $F(x) = 0$ genügen kann, und dieser Wert reduciert sich auf eine reelle Gröfse, wenn $\beta = 0$ ist.

Im Allgemeinen aber mufs x von der Form $\alpha + \beta\sqrt{-1}$ vorausgesetzt werden. Dies liefert einen neuen Beweis des auf die Form der imaginären Wurzeln der Gleichungen bezüglichen Satzes, einen Beweis, der für alle Arten von algebraischen und transcendenten Gleichungen gilt.

§ 15.

Auflösung der unbestimmten Gleichung $Ly^n + My^{n-1}z + Ny^{n-2}z^2 + \cdots + Vz^n = \pm H$ in ganzen Zahlen.

120.

Wir setzen voraus, dafs diese Gleichung auf die in No. 75 angegebene Weise vorbereitet ist, und dafs man somit y und z und ebenso auch z und H als zu einander prim betrachten kann. Dies vorausgeschickt, setzen wir analog:

$$y = \vartheta z + Hu,$$

wo ϑ eine zwischen $-\frac{1}{2}H$ und $+\frac{1}{2}H$ liegende Zahl ist, substituieren diesen Wert in die gegebene Gleichung und dividieren das Ganze durch H. Dies giebt:

$$\begin{aligned}\pm 1 = {} & \frac{L\vartheta^n + M\vartheta^{n-1} + N\vartheta^{n-2} + \cdots + V}{H} z^n \\ & + (nL\vartheta^{n-1} + (n-1)M\vartheta^{n-2} + \cdots) z^{n-1}u \\ & + \left(\frac{n(n-1)}{2} L\vartheta^{n-2} + \frac{(n-1)(n-2)}{2} M\vartheta^{n-3} + \cdots\right) Hz^{n-2}u^2 \\ & + \cdots\end{aligned}$$

Da jedoch z und H prim zu einander sind, so kann diese Gleichung nicht bestehen, wofern nicht

$$\frac{L\vartheta^n + M\vartheta^{n-1} + N\vartheta^{n-2} + \cdots + V}{H}$$

eine ganze Zahl ist. Dies ist die Bedingung, welche zur Bestimmung von ϑ dient. Man versuche also für ϑ der Reihe nach alle ganzen Zahlen zwischen $-\frac{1}{2}H$ und $+\frac{1}{2}H$. Giebt es unter diesen keine, für welche $L\vartheta^n + M\vartheta^{n-1} + N\vartheta^{n-2} + \cdots$ durch H teilbar ist, so folgt daraus mit Gewifsheit, dafs die gegebene Gleichung nicht in ganzen Zahlen auflösbar ist. Findet man aber eine oder mehrere Zahlen, welche dieser Bedingung Genüge leisten, so hat

man weiter für jeden Wert von ϑ die transformierte Gleichung in z und u, welche von der Form ist:

$$az^n + bz^{n-1}u + cz^{n-2}u^2 + \cdots + ku^n = \pm 1$$

aufzulösen, und es ist ersichtlich, daſs jede ganzzahlige Lösung dieser eine ebensolche Lösung der gegebenen Gleichung zur Folge hat.

Mithin reduciert sich alles darauf, eine Gleichung aufzulösen, welche dieselbe Form besitzt, wie die gegebene Gleichung, in welcher aber die rechte Seite gleich ± 1 ist.

Man darf voraussetzen, daſs die linke Seite der gegebenen Gleichung (auch bevor man irgend eine Reduction darauf anwendet) nicht durch einen rationalen Faktor teilbar ist. Denn wenn sie sich in zwei derartige Faktoren, deren einer vom Grade m, deren anderer vom Grade $n - m$ sei, zerlegen lieſse, so würde die gegebene Gleichung in zwei andere zerfallen von der Form:

$$L'y^m + M'y^{m-1}z + N'y^{m-2}z^2 + \cdots = \pi$$
$$L''y^{n-m} + M''y^{n-m-1}z + N''y^{n-m-2}z^2 + \cdots = \frac{H}{\pi},$$

wo π ein Teiler von H ist. Es würde daher die Aufgabe eine vollkommen bestimmte sein.

Aus dieser Annahme folgt offenbar, daſs die linke Seite der transformierten Gleichung, nämlich $az^n + bz^{n-1}u + cz^{n-2}u^2 + \cdots$ ebenfalls nicht mehr in rationale Faktoren zerlegbar ist. Mithin giebt es keine ganzzahligen Werte von u und z, für welche diese linke Seite gleich Null werden könnte, und es ist somit ± 1 der **absolut kleinste** Wert von allen, welche sie annehmen kann, wenn man für y und z irgend welche positive oder negative ganze Zahlen setzt.

121.

Nachdem wir dieses festgestellt haben, wollen wir allgemein untersuchen, welches die Werte von t und u sein müssen, damit die homogene Funktion

$$at^n + bt^{n-1}u + ct^{u-2}u^2 + \cdots + ku^n$$

möglichst klein werde.

Dazu denken wir uns, daſs wir durch Auflösung der bestimmten Gleichung

$$0 = ax^n + bx^{n-1} + cx^{n-2} + \cdots + k$$

die einfachen reellen Faktoren

$$x - \alpha, \qquad x - \alpha', \qquad x - \alpha'', \ldots$$

und die doppelten imaginären Faktoren
$$(x-\beta)^2+\gamma^2, \qquad (x-\beta')^2+\gamma'^2, \ldots$$
gefunden haben. Alsdann ist die gegebene Funktion
$$at^n + bt^{n-1}u + ct^{n-2}u^2 + \cdots,$$
die wir mit $F(t, u)$ bezeichnen, gleich dem Produkte:
$$a(t-\alpha u)(t-\alpha' u)(t-\alpha'' u)\ldots\big((t-\beta u)^2+\gamma^2u^2\big)\big((t-\beta' u)^2+\gamma'^2u^2\big)\ldots$$
Nehmen wir nun an, daſs die Werte von t und u, welche dem Minimum dieser Funktion entsprechen, $t=p$ und $u=q$ seien, so daſs dieses Minimum gleich
$$F(p,q)=a(p-\alpha q)(p-\alpha' q)\ldots\big((p-\beta q)^2+\gamma^2q^2\big)\ldots$$
ist, so muſs also, wenn man für t und u ganzzahlige Werte setzt, die (wenigstens bis zu einer gewissen Grenze) von p und q verschieden sind,
$$F(p,q)<F(t,u)$$
sein. Dies könnte nicht stattfinden, wenn jeder Faktor von $F(t, u)$ gleich oder kleiner als der entsprechende Faktor von $F(p, q)$ wäre. Es muſs also wenigstens einen Faktor von $F(t, u)$ geben, der gröſser als der entsprechende Faktor von $F(p, q)$ ist. Dieser Faktor kann entweder zu den einfachen reellen Faktoren, oder zu den doppelten imaginären Faktoren gehören.

1) Es sei $t-\alpha u$ der einfache Faktor, welcher gröſser ist als der ihm entsprechende $p-\alpha q$. Da t und u willkürlich angenommen sind, und da man somit voraussetzen kann, daſs $\frac{t}{u}$ nur sehr wenig von $\frac{p}{q}$ verschieden ist, so folgt daraus, daſs $\frac{p}{q}$ ein sehr nahe bei α liegender Bruch sein muſs, und man kann sogar hieraus schlieſsen, daſs $\frac{p}{q}$ einer der Näherungsbrüche der Wurzel α ist. Sind nämlich $\frac{p^0}{q^0}$, $\frac{p}{q}$, $\frac{p'}{q'}$ drei aufeinanderfolgende Näherungsbrüche von α, so ist in No. 8 gezeigt worden, daſs, welches auch die Zahlen t und u sein mögen, wofern nur u kleiner als q' ist, stets die Gröſse $t-\alpha u$ gröſser ist als $p-\alpha q$, was der angegebenen Bedingung entspricht.

2) Es sei $(t-\beta u)^2+\gamma^2u^2$ der doppelte imaginäre Faktor, welcher gröſser ist als der ihm entsprechende $(p-\beta q)^2+\gamma^2q^2$. Setzen wir voraus, daſs $u<q$ genommen sei, so wird um so mehr $t-\beta u$ gröſser als $p-\beta q$ sein. Dies findet aber statt, wenn $\frac{p}{q}$

einer der Näherungsbrüche der Gröfse β, des reellen Teils der imaginären Wurzel $\beta \pm \gamma \sqrt{-1}$, ist.

122.

Wir kehren zur Betrachtung des ersten Falles zurück und nehmen an, dafs man $t = p^0$, $u = q^0$ genommen habe, wo $\frac{p^0}{q^0}$ der Näherungsbruch ist, welcher $\frac{p}{q}$ vorangeht und durch Entwicklung dieses letzteren Bruches in einen Kettenbruch gegeben wird. Dann mufs also $p^0 - \alpha q^0$ gröfser als $p - \alpha q$, oder es mufs $\frac{p^0 - \alpha q^0}{p - \alpha q}$ gröfser als 1 sein. Im Übrigen kann aber diese Gröfse positiv oder negativ sein.

Ist zunächst $\frac{p^0 - \alpha q^0}{p - \alpha q} = -y$, so folgt daraus $\alpha = \frac{py + p^0}{qy + q^0}$. Da nun y positiv und gröfser als 1 ist, so werden $\frac{p^0}{q^0}$ und $\frac{p}{q}$ zwei aufeinanderfolgende Näherungsbrüche von α und y der dem zweiten entsprechende vollständige Quotient sein.

Ist zweitens $\frac{p^0 - \alpha q^0}{p - \alpha q} = +y$, so hat man $\alpha = \frac{py - p^0}{qy - q^0}$. Jedoch mufs man diesen Fall in zwei zerlegen, je nachdem $y > 2$ oder < 2 ist.

Hat man $y > 2$, so setze man $y = 1 + z$, wo $z > 1$ ist. Dann erhält man:

$$z = \frac{pz + p - p^0}{qz + q - q^0}.$$

Mithin werden $\frac{p - p^0}{q - q^0}$ und $\frac{p}{q}$ ebenfalls zwei aufeinanderfolgende Näherungsbrüche von α und z der dem letzteren entsprechende vollständige Quotient sein.

In diesen ersten Fällen, welche bereits einen grofsen Umfang haben, ist also auf eine direkte und sehr einfache Weise gezeigt worden, dafs $\frac{p}{q}$ ein Näherungsbruch der Wurzel α ist.

Es bleibt der letzte Fall, in welchem $y < 2$ ist, zu untersuchen übrig. Ist alsdann $y = 1 + \frac{1}{z}$, wo z stets gröfser als 1 ist, so hat man:

$$\alpha = \frac{(p - p^0)\, z + p}{(q - q^0)\, z + q} = \frac{(p - p^0)(z + 1) + p^0}{(q - q^0)(z + 1) + q^0}.$$

Mithin sind $\frac{p^0}{q^0}$ und $\frac{p - p^0}{q - q^0}$ zwei aufeinanderfolgende Näherungs-

brüche von α*) und der dem letzteren entsprechende vollständige Quotient ist $z + 1$, eine Gröfse, die gröfser ist als 2.

Der Quotient dürfte aber nur gleich $1 +$ einem Bruche sein, damit $\frac{p}{q}$ der auf $\frac{p - p^0}{q - q^0}$ folgende Näherungsbruch wäre. Da man nun $z + 1 > 2$ hat, so folgt, dafs in diesem letzteren Falle $\frac{p}{q}$ kein Näherungsbruch von α sein kann. Indessen sieht man wenigstens, dafs, weil $\frac{p - p^0}{q - q^0}$ ein solcher ist, und der Unterschied zwischen $\frac{p}{q}$ und $\frac{p - p^0}{q - q^0}$ nur $\frac{1}{q(q - q^0)}$ beträgt, $\frac{p}{q}$ jedenfalls immer ein sehr angenäherter Wert der Wurzel α ist.

Ist $p - p^0 = \pi$, $q - q^0 = \varphi$, so können wir durch $\frac{p^0}{q^0}$, $\frac{\pi}{\varphi}$, $\frac{\pi'}{\varphi'}$ drei aufeinanderfolgende Näherungsbrüche von α darstellen, und da q zwischen φ und φ' fällt, so hat man offenbar (No. 8):

$$p - \alpha q > \pi - \alpha\varphi.$$

Setzt man aber $t = \pi$, $u = \varphi$, so mufs $F(\pi, \varphi) > F(p, q)$ sein, da das letztere ein Minimum ist. Mithin mufs es in dem Werte von $F(\pi, \varphi)$ irgend einen andern Faktor $\pi - \alpha'\varphi$ geben, der gröfser ist als der entsprechende Faktor $p - \alpha' q$.

Weil nun $\frac{\pi - \alpha'\varphi}{p - \alpha' q}$ gröfser als 1 ist und im Übrigen positiv oder negativ sein kann, so schliefst man wie oben, dafs $\frac{p}{q}$ ein Näherungsbruch von α' oder wenigstens

$$\alpha' = \frac{(p - \pi)(z + 1) + \pi}{(q - \varphi)(z + 1) + \varphi},$$

wo z positiv und > 1, ist. Daraus folgt, indem man die Werte von π und φ einsetzt:

$$\alpha' = \frac{p^0(z + 1) + p - p^0}{q^0(z + 1) + q - q^0} = \frac{p^0 z + p}{q^0 z + q} = \frac{p^0(z + \mu^0) + p^{00}}{q^0(z + \mu^0) + q^{00}}$$

(man nimmt nämlich stets $p = \mu^0 p^0 + p^{00}$ an). Mithin werden $\frac{p^{00}}{q^{00}}$, $\frac{p^0}{q^0}$ zwei aufeinanderfolgende Näherungsbrüche von α' sein und der folgende Bruch wird sein:

---

*) Es wird $p - p^0 > p^0$ angenommen. In der That ergiebt die Kettenbruchentwicklung von $\frac{p}{q}$ eine Reihe von Quotienten, deren letzter nach Belieben gröfser als 1 oder gleich 1 angenommen werden kann. Nimmt man ihn gröfser als 1, so kann p nicht kleiner sein als $2p^0 + p^{00}$, und man hat daher $p - p^0 > p^0$. Anm. d. Verf.

$$\frac{p^0(k+\mu^0)+p^{00}}{q^0(k+\mu^0)+q^{00}} \text{ oder } \frac{p^0k+p}{q^0k+q},$$

wo k die gröſste in z enthaltene ganze Zahl ist. Und da q zwischen q^0 und q^0k+q liegt, so ergiebt sich, daſs $p^0-\alpha'q^0 < p-\alpha'q$ ist.

Dasselbe Schluſsverfahren kann man auf die andern Wurzeln α'', α''', ... und selbst auf die Gröſsen β, β', β'', ... anwenden. Es folgt daraus der allgemeine Schluſs, daſs der Bruch $\frac{p}{q}$, welcher dem Minimum der gegebenen Funktion entspricht, unter den Näherungsbrüchen einer der Wurzeln α, α', α'', ... oder einer der Gröſsen β, β', β'' ... enthalten sein muſs. Ist er nämlich nicht darunter enthalten, so müssen die folgenden Bedingungen zusammen stattfinden:

1) die Gröſse $\frac{p^0-\alpha q^0}{p-\alpha q}$, welche sich auf eine bestimmte Wurzel α bezieht, muſs zwischen $+1$ und $+2$ liegen.

2) Alle analogen Gröſsen

$$\frac{p^0-\alpha'q^0}{p-\alpha'q}, \frac{p^0-\alpha''q^0}{p-\alpha''q}, \ldots \frac{p^0-\beta q^0}{p-\beta q}, \frac{p^0-\beta'q^0}{p-\beta'q}, \ldots,$$

welche sich auf die andern Wurzeln beziehen, müssen kleiner als 1 sein.

Wenn aber auch dieses der Fall ist, so ist es doch unmöglich, daſs die Gröſse $\frac{F(p^0,q^0)}{F(p,q)}$, welche aus dem Produkte aller Faktoren

$$\frac{p^0-\alpha q^0}{p-\alpha q}, \frac{p^0-\alpha'q^0}{p-\alpha'q}, \frac{p^0-\alpha''q^0}{p-\alpha''q}, \ldots \frac{(p^0-\beta q^0)^2+\gamma^2 q^{0\,2}}{(p-\beta q)^2+\gamma^2 q^2}, \ldots$$

besteht, gröſser als 1 ist, wie es der Fall sein müſste, wenn $F(p,q)$ ein Minimum ist.

Da nämlich die Differenz zwischen $\frac{p}{q}$ und $\frac{p^0}{q^0}$ nur $\frac{1}{qq^0}$ beträgt, und da $\frac{p^0}{q^0}$ ein Näherungsbruch von α ist, so braucht es unter den Wurzeln α', α'', ... und den Gröſsen β, β', ... nur eine zu geben, die entweder entgegengesetztes Zeichen besitzt wie α, oder deren Differenz mit α merklich gröſser ist als $\frac{1}{qq^0}$. Ist alsdann α' diese Wurzel, so wird der Faktor $\frac{p^0-\alpha'q^0}{p-\alpha'q}$ ziemlich nahe gleich $\frac{q^0}{q}$ und somit kleiner als $\frac{1}{2}$ sein; und ist β eine von α hinreichend verschiedene Gröſse, so wird der Faktor $\frac{(p^0-\beta q^0)^2+\gamma^2 q^{0\,2}}{(p-\beta q)^2+\gamma^2 q^2}$ sich ebenfalls sehr nahe auf $\left(\frac{q^0}{q}\right)^2$ reducieren und demnach kleiner als $\frac{1}{4}$ sein. Mithin würde es in dem Werte von $\frac{F(p^0,q^0)}{F(p,q)}$ nur einen Faktor

geben, der gröfser als die Einheit aber kleiner als 2 ist, während alle übrigen Faktoren kleiner als 1 wären und unter diesen sich wenigstens einer fände, der kleiner als $\frac{1}{2}$ oder sogar kleiner als $\frac{1}{4}$ wäre. Folglich würde die Gröfse $\frac{F(p^0, q^0)}{F(p, q)}$ kleiner als 1 sein. Dies ist aber gegen die gemachte Annahme, dafs $F(p, q)$ ein Minimum sein solle. Mithin ist schliefslich*) der Bruch $\frac{p}{q}$ immer ein Näherungsbruch einer der Gröfsen $\alpha, \alpha', \alpha'', \ldots, \beta, \beta', \beta'', \ldots$

123.

Die soeben bewiesene Bedingung bestimmt noch nicht das gesuchte Minimum; sie giebt nur eine Reihe von Gröfsen an, unter denen der Bruch $\frac{p}{q}$ zu suchen ist, welcher die Eigenschaft besitzt, das Minimum zu liefern. Das Verfahren, welches man einschlagen mufs, ist demnach folgendes:

Man entwickle der Reihe nach jede der reellen Wurzeln α der Gleichung $ax^n + bx^{n-1} + \cdots + k = 0$ in einen Kettenbruch.

Ebenso entwickle man von den imaginären Wurzeln derselben Gleichung die reellen Teile in Kettenbrüche.

Für $\frac{p}{q}$ nehme man der Reihe nach alle Näherungsbrüche, welche sich bei diesen verschiedenen Rechnungen ergeben, und setze die Werte von p und q in die gegebene Funktion ein. Dadurch erhält man ebenso viele Resultate, die jedes für sich eine Art von Minimum sind. Das kleinste von allen diesen Resultaten oder das absolute Minimum wird dann dasjenige sein, welches bestimmt werden sollte.

124.

Bemerkung 1.

Wenn die reelle Wurzel α oder der reelle Teil β einer imaginären Wurzel negativ ist, so führe man die Entwicklung in einen Kettenbruch ebenso aus, als ob sie positiv wären, gebe aber sodann jedem Näherungsbruche das Zeichen —, bevor man ihn für $\frac{p}{q}$ nimmt.

---

*) Man findet diesen Satz in den Zusätzen zu Euler's Algebra No. 28; jedoch ist der gelehrte Verfasser nicht auf die Einzelheiten des Beweises eingegangen. Einen solchen hat er für den Fall, wo das Minimum 1 ist, in den Abhandlungen der Berliner Akademie vom Jahre 1768 gegeben; indessen besteht in Bezug auf die Gröfsen $\beta, \beta', \ldots$ einige Verschiedenheit im Wortlaut des Satzes. Anm. d. Verf.

Hier drängt sich die Frage auf, welches der beiden Glieder p und q negativ zu nehmen ist. Diese Frage ist leicht zu beantworten. Ist der Exponent n der gegebenen Gleichung eine gerade Zahl, so ist es gleichgültig, welches der beiden Glieder p und q man mit dem Zeichen — versieht, da die Gröfse $ap^n + bp^{n-1}q + \cdots$ vollständig dieselbe bleibt. Ist dagegen der Exponent n eine ungerade Zahl, so wird die Gröfse $ap^n + bp^{n-1}q + \cdots$ denselben Wert behalten, aber ihr Zeichen ändern, wenn man einmal p positiv und q negativ, das andere Mal p negativ und q positiv nimmt, oder allgemein, wenn man zu gleicher Zeit die Vorzeichen von p und q ändert.

Man sieht hieraus, dafs im Falle eines **ungeraden** n die beiden Gleichungen

$$ap^n + bp^{n-1}q + \cdots + kq^n = + H$$

und

$$ap^n + bp^{n-1}q + \cdots + kq^n = - H$$

stets gleichzeitig auflösbar sind.

125.

Bemerkung 2.

Entwickelt man jede Wurzel α nach der oben (No. 100) auseinandergesetzten Methode in einen Kettenbruch, so kann man sich der Mühe überheben, den Wert von $F(p, q)$ für jeden Näherungsbruch $\frac{p}{q}$ zu berechnen. Denn ist die transformierte Gleichung, welche dem Näherungsbruche $\frac{p}{q}$ entspricht, die folgende:

$$Az^n + Bz^{n-1} + \cdots = 0,$$

so ist der erste Koefficient A dieser transformierten Gleichung genau der Wert von $F(p, q)$. Man braucht also nur auf das erste Glied jeder transformierten Gleichung zu achten, um das verlangte Minimum zu erhalten.

Dasselbe würde hinsichtlich der Gröfsen β stattfinden, wenn man ihre Entwicklung mittelst der Gleichung, deren reelle Wurzeln sie sind, ausführte. Da aber diese Gleichung in der Regel von einem zu hohen Grade ist, so ist es besser, diese Entwicklung mit Hülfe eines Näherungswertes von β auszuführen und alsdann für $\frac{p}{q}$ die daraus entstehenden Näherungsbrüche (No. 114) einzusetzen. Übrigens wird man sogleich sehen, dafs die Entwicklung dieser Gröfsen nur bis zu einer bestimmten Grenze fortgesetzt zu werden braucht.

126.

Bemerkung 3.

Die angegebenen Rechnungen sind dieselben, mag nun das Minimum bereits bestimmt sein, wie dies der Fall ist, wenn man die Gleichung $at^n + bt^{n-1}u + ct^{n-2}u^2 + \cdots + ku^n = \pm 1$ auflösen will, oder mag man einfach suchen, welches der kleinste Wert ist, den die linke Seite dieser Gleichung annehmen kann. Im ersten Falle begreift man wohl ohne weiteres, daſs das Problem nicht immer auflösbar ist; im zweiten Falle hat man nichts weiter zu thun, als unter mehreren Reihen bekannter Zahlen die kleinste Zahl herauszusuchen.

Da aber in beiden Fällen die Berechnung der Entwicklung sich ins Unendliche erstreckt, und da man über den zweiten Grad hinaus kein Gesetz kennt, welchem die aufeinanderfolgenden Quotienten und transformierten Gleichungen unterworfen wären, so hat man offenbar das Minimum der Funktion $at^n + bt^{n-1}u + \cdots + ku^n$ nur unter der Annahme bestimmt, daſs t und u den gröſsten Zähler und Nenner der berechneten Näherungsbrüche nicht übersteigen. Man kann also nicht behaupten, daſs ein gleiches oder selbst kleineres (wenn es nicht schon ± 1 ist) Minimum nicht eintreten könnte für weitere Näherungsbrüche, deren Zähler und Nenner noch gröſser sind. In der That sieht man keinen Hinderungsgrund dafür, daſs nicht auch bei sehr groſsen Werten von p und q die Funktion $ap^n + bp^{n-1}q + \cdots$ sich auf 1 oder auf eine sehr kleine Zahl reducieren könnte, so daſs es scheint, als ob man in dieser Hinsicht keine Grenze angeben kann.

Wir bemerken jedoch, daſs eine solche Unbestimmtheit hinsichtlich der Gröſse der Zahlen p und q nicht stattfinden kann bei den Näherungsbrüchen, welche aus der Entwicklung des reellen Teiles β einer imaginären Wurzel $\beta + \gamma\sqrt{-1}$ hervorgehen. Denn ein solcher Faktor wie $(p - \beta q)^2 + \gamma^2 q^2$ kann nur bis zu einem gewissen Punkte abnehmen, nämlich so lange die Abnahme des Teiles $(p - \beta q)^2$ beträchtlicher ist als die Zunahme des andern Teiles $\gamma^2 q^2$. Bald nachher aber müssen diese Faktoren schnell zunehmen. Deshalb sieht man, daſs es nicht notwendig ist, die Gleichungen, deren Wurzeln $\beta, \beta', \ldots$ sind, zu suchen, sondern daſs man sich, wie schon erwähnt, mit einem Näherungswerte dieser Gröſsen begnügen kann.

127.

Wir wollen annehmen, daſs $\frac{p}{q}$ ein der Wurzel α hinreichend nahekommender Näherungsbruch sei, so daſs die

Differenz $\frac{p}{q} - \alpha$ viel kleiner sei als die Differenz zwischen der Wurzel α und jeder der andern Wurzeln oder reellen Teile der Wurzeln α', α'', ... β, β', ... Setzt man dann zur Abkürzung:

$$L = (\alpha - \alpha')(\alpha - \alpha'') \cdots \left((\alpha - \beta)^2 + \gamma^2\right) \left((\alpha - \beta')^2 + \gamma'^2\right) \cdots,$$

so hat man sehr nahe:

$$F(p, q) = a q^{n-1} (p - \alpha q) L.$$

Ist z der dem Näherungsbruche $\frac{p}{q}$ entsprechende vollständige Quotient, so ist:

$$p - \alpha q = \pm \frac{1}{qz + q^0},$$

mithin:

$$F(p, q) = \pm a L \frac{q^{n-2}}{z + \frac{q^0}{q}}.$$

Da in dieser Formel aL eine konstante Gröfse ist, so sieht man, dafs, wenn $F(p, q)$ eine gegebene Zahl sein soll, der Quotient z im Allgemeinen mit q^{n-2} proportional sein mufs.

Will man also z. B., dafs sich $F(p, q)$ auf ± 1 reduciere, wie dies in den vorgelegten Gleichungen notwendig ist, so mufs nahezu

$$z = a L q^{n-2}$$

sein. Dies ist die Gröfse der Quotienten, aus denen man die Näherungsbrüche erkennt, welche der Bedingung des Minimums

$$F(p, q) = \pm 1$$

genügen. Diese Formel ist besonders dann von Nutzen, wenn die Entwicklung einer Wurzel nicht nach der Methode der aufeinanderfolgenden transformierten Gleichungen, sondern mit Hülfe eines Näherungswertes dieser Wurzel (No. 112) vorgenommen wird.

In dem Mafse, wie das Entwicklungsverfahren fortschreitet, nimmt der Wert von q und demnach der von z (denn man setzt hier $n > 2$ voraus) zu, so dafs es immer weniger wahrscheinlich wird, dafs man den für das Minimum erforderlichen Quotienten z finden werde. Wenn jedoch die Wurzel α von einer oder mehreren andern Wurzeln α', α'', ... oder von den Gröfsen β, β', ... nur sehr wenig verschieden ist, so kann die Grenze L äufserst klein werden, und es wird nicht mehr ein ebenso beträchtlicher Quotient z erforderlich sein, um das Minimum von $F(p, q)$ zu erhalten. Diese Bemerkung steht mit den bereits auseinandergesetzten Eigenschaften (No. 109 und 110) im Einklang.

Nimmt man zweitens an, dafs $\frac{p}{q}$ einer der Näherungsbrüche der Gröfse β sei, setzt man ferner voraus, dafs die Differenz zwischen $\frac{p}{q}$ und β um vieles kleiner sei als γ und ebenso um vieles kleiner als irgend eine der Gröfsen α, α', α'', ... β', β'', ..., und macht man zur Abkürzung:

$$\Delta = (\beta - \alpha)(\beta - \alpha')(\beta - \alpha'') \cdots \left((\beta - \beta')^2 + \gamma'^2\right) \cdots,$$

so erhält man nahezu:

$$F(p, q) = aq^n\gamma^2\Delta.$$

Soll also $F(p, q) = \pm 1$ sein, so mufs man

$$q^n = \pm \frac{1}{a\gamma^2\Delta}$$

haben; mithin kann q nicht gröfser sein als $\sqrt[n]{\frac{1}{a\gamma^2\Delta}}$, woraus hervorgeht, dafs das Minimum ± 1 mit Hülfe der imaginären Wurzeln nur in sehr beschränkten Fällen eintreten kann, sobald γ oder Δ sehr klein sind, d. h. sobald nahezu gleiche Wurzeln vorhanden sind. Zu gleicher Zeit erhält man die Grenze des Nenners q, über welche hinaus es überflüssig ist, die Entwicklung der Gröfse β sowie das Probieren mit den daraus sich ergebenden Näherungsbrüchen fortzusetzen.

Wir haben bereits im vorhergehenden Paragraphen Beispiele für die Auflösung der homogenen unbestimmten Gleichungen, deren rechte Seite ± 1 ist, gegeben; wir begnügen uns daher, ein neues Beispiel hinzuzufügen, in welchem eine Lösung durch die reelle Wurzel, eine andere durch die imaginären Wurzeln gegeben wird.

128.

Beispiel.

Es sei die Aufgabe gestellt, das Minimum der Funktion

$$7t^3 - 110t^2u + 565tu^2 - 941u^3$$

zu finden.

Betrachtet man die Gleichung:

$$7x^3 - 110x^2 + 565x - 941 = 0,$$

so findet man, dafs dieselbe eine reelle Wurzel zwischen 3 und 4 und zwei nur wenig von einander verschiedene imaginäre Wurzeln besitzt.

Folgendes ist die Kettenbruchentwicklung der reellen Wurzel:

$7x^3 - 110x^2 + 565x - 941 = 0$	3	1 : 0
$-47z^3 + 94z^2 - 47z + 7 = 0$	1	3 : 1
$7z^3 - 47z - 47 = 0$	2	4 : 1
$-85z^3 + 37z^2 + 42z + 7 = 0$	1	11 : 3
$z^3 - 139z^2 - 218z - 85 = 0$	140	15 : 4
$-11005z^3 + 19662z^2 + 281z + 1 = 0$	1	2111 : 563
$8939z^3 + 6590z^2 - 13353z - 11005 = 0$	1	2126 : 567
$-8829z^3 + 26644z^2 + 33407z + 8939 = 0$	4	4237 : 1130
$3807z^3 - 177233z^2 - 79304z - 8829 = 0$	46	19074 : 5087
$-8123689z^3 + 7782096z^2 + 348133z + 3807 = 0$	1	877404 : 235132
$10347z^3 - 8458742z^2 - 16588971z - 8123689 = 0$	819	896478 : 240219
u. s. w.	2	u. s. w.
	6	
	2	
	u. s. w.	

Aus den ersten Gliedern der transformierten Gleichungen sieht man, dafs das Minimum $+1$ stattfindet, sobald $t = 15$ und $u = 4$ ist, so dafs diese Werte der Gleichung genügen:

$$7t^3 - 110t^2u + 565tu^2 - 941u^3 = 1.$$

In der weiteren Rechnung findet man keine transformierten Gleichungen mehr, deren erstes Glied den Koefficienten 1 hat. Demnach ist man sicher, dafs die erste Wurzel keine andere Lösung der vorstehenden Gleichung liefert, wofern man nicht die Zahl u viel gröfser als $819 . 240219$ annimmt; aber gerade wegen dieser Gröfse erscheint es wenig wahrscheinlich, dafs die Fortsetzung der Rechnung neue Werte von t und u liefern werde.

Man hat daher nur noch den reellen Teil der imaginären Wurzeln in einen Kettenbruch zu entwickeln. Da nun aber die Gleichung nur vom dritten Grade ist, so wird, wenn man mit α die reelle Wurzel, deren angenäherten Wert wir soeben gefunden haben, bezeichnet, der reelle Teil β der imaginären Wurzeln der folgende sein:

$$\beta = \frac{110}{14} - \frac{1}{2}\alpha.$$

Setzt man den bekannten Wert von α ein, und entwickelt man das Resultat in einen Kettenbruch, so erhält man folgende Quotienten und Näherungsbrüche:

Quotienten: 5, 1, 55, 1, 2, 2, 1, 3

Näherungsbrüche: $\frac{1}{0}$, $\frac{5}{1}$, $\frac{6}{1}$, $\frac{335}{56}$, $\frac{341}{57}$, ...

Nimmt man nun nach und nach für $\frac{t}{u}$ diese verschiedenen Näherungsbrüche, so findet man, dafs die Werte $t = 6$, $u = 1$ ebenfalls das Minimum $+1$ ergeben und somit eine zweite Lösung der unbestimmten Gleichung

$$7t^3 - 110t^2u + 565tu^2 - 941u^3 = 1$$

liefern. Es würde überflüssig sein, für $\frac{t}{u}$ andere Näherungsbrüche zu nehmen, da die oben gefundene Grenze

$$q = \sqrt[n]{\frac{1}{a\gamma^2 A}}$$

nahezu $q = 1$ ergiebt.

Zweiter Hauptteil.

Allgemeine Eigenschaften der Zahlen.

§ 1.

Sätze über die Primzahlen.

129.

Satz. Ist c eine Primzahl und N eine beliebige durch c nicht teilbare Zahl, so ist die Gröfse $N^{c-1} - 1$ durch c teilbar, so dafs man erhält:

$$\frac{N^{c-1} - 1}{c} = \text{ganze Zahl} = e^{*}).$$

Ist x eine beliebige ganze Zahl, und betrachtet man die bekannte Formel:

$$(1 + x)^c = 1 + cx + \frac{c(c-1)}{1 \cdot 2} x^2 + \frac{c(c-1)(c-2)}{1 \cdot 2 \cdot 3} x^3 + \cdots + cx^{c-1} + x^c,$$

so sieht man leicht, dafs alle Glieder dieser Reihe, mit Ausnahme des ersten und des letzten, durch c teilbar sind. Ist nämlich M der Koefficient von x^m, so hat man:

$$M = \frac{c(c-1)(c-2) \cdots (c-m+1)}{1 \cdot \ 2 \cdot \ \ 3 \ \cdots \ \ m}$$

oder:

$$M \cdot 1 \cdot 2 \cdot 3 \cdots m = c(c-1)(c-2) \cdots (c-m+1).$$

Da nun die rechte Seite durch c teilbar ist, so mufs es auch die linke sein, und da der Exponent m in den in Frage kommenden Gliedern nicht gröfser ist als $c - 1$, so kann c, welches als Primzahl vorausgesetzt ist, nicht in dem Produkte $1 . 2 . 3 \ldots m$ aufgehen. Es

*) Diesen Satz, einen der hauptsächlichsten in der Zahlentheorie, verdankt man Fermat. Ein Beweis dafür ist von Euler an verschiedenen Stellen der Abhandlungen der Petersburger Akademie und besonders im 1. Bande der „Novi Commentarii“ gegeben worden. Anm. d. Verf.

mufs daher notwendig für jeden Wert von $m = 1$ bis $m = c - 1$ in M aufgehen. Mithin ist die Gröfse

$$(1 + x)^c - 1 - x^c$$

teilbar durch c, welches auch die ganze Zahl x sein möge.

Ist jetzt $1 + x = N$, so geht die vorstehende Gröfse über in:

$$N^c - (N - 1)^c - 1.$$

Da diese teilbar ist durch c, so erhält man, wenn die Vielfachen von c fortgelassen werden:

$$N^c - 1 = (N - 1)^c$$

oder:

$$N^c - N = (N - 1)^c - (N - 1).$$

Setzt man jetzt $N - 1$ für N und läfst stets die Vielfachen von c aufser Acht, so wird analog:

$$(N - 1)^c - (N - 1) = (N - 2)^c - (N - 2).$$

Fährt man in dieser Weise fort, indem man immer von gleichen Resten zu gleichen Resten übergeht, so gelangt man notwendig zu dem Reste $(N - N)^c - (N - N)$, der offenbar gleich 0 ist. Demnach sind auch alle vorhergehenden Reste gleich 0, und somit ist $N^c - N$ teilbar durch c.

Da aber $N^c - N$ das Produkt aus N und $N^{c-1} - 1$ ist und da N nach Voraussetzung nicht teilbar ist durch c, so mufs $N^{c-1} - 1$ durch c teilbar sein, w. z. b. w.

Zusatz. Ist c eine Primzahl, so kann man der Gleichung

$$\frac{x^{c-1} - 1}{c} = e$$

Genüge leisten, indem man für x eine beliebige durch c nicht teilbare Zahl setzt. Betrachtet man daher nur diejenigen Werte von x, welche positiv und kleiner als c sind, so sind diese Werte die aufeinanderfolgenden Zahlen $1, 2, 3, 4, \ldots c - 1$. Betrachtet man aber diejenigen Werte oder Lösungen, welche zwischen $-\frac{1}{2}c$ und $+\frac{1}{2}c$ liegen, so sind diese Werte oder Lösungen:

$$\pm 1, \ \pm 2, \ \pm 3, \cdots \pm \frac{c-1}{2}.$$

In beiden Fällen ist die Anzahl der Lösungen der in Rede stehenden Gleichung gleich $c - 1$, also gleich dem Exponenten von x.

130.

Satz. Ist n eine Primzahl, so ist das Produkt

$$1 . 2 . 3 \ldots (n - 1)$$

vermehrt um 1 durch n teilbar.

Aus der Differenzenrechnung ergiebt sich nämlich, dafs für jede ganze Zahl m die Gleichung besteht:

$$1 \cdot 2 \cdot 3 \cdots m = m^m - \frac{m}{1}(m-1)^m + \frac{m(m-1)}{1 \cdot 2}(m-2)^m - \frac{m(m-1)(m-2)}{1 \cdot 2 \cdot 3}(m-3)^m + \cdots$$

Setzt man $m = n - 1$, und läfst man die Vielfachen von n aufser Acht, so erhält man dem vorhergehenden Satze zufolge:

$$m^m = 1, \quad (m-1)^m = 1, \quad (m-2)^m = 1, \ldots$$

Mithin reduciert sich das Produkt $1 . 2 . 3 \ldots m$, wenn man dieselben Gröfsen wegläfst, auf:

$$1 - m + \frac{m(m-1)}{1 \cdot 2} - \frac{m(m-1)(m-2)}{1 \cdot 2 \cdot 3} + \cdots,$$

wobei die Anzahl der Glieder dieser Reihe gleich m ist. Nun bilden aber diese m Glieder die Entwicklung der Potenz $(1-1)^m$, vermindert um das letzte Glied derselben, welches $+1$ ist, da m eine gerade Zahl ist. Mithin ist die Summe der in Frage kommenden Glieder $= (1-1)^m - 1 = -1$. Es ist daher die Gröfse $1 . 2 . 3 \ldots (n-1) + 1$ durch n teilbar.

131.

Dieser Satz, dessen Waring in seinen Meditationes algebraicae Erwähnung thut, und dessen Entdeckung er Jean Wilson zuschreibt, wurde zuerst von Lagrange in den Abhandlungen der Berliner Akademie vom Jahre 1771 und sodann von Euler in seinen Opuscula analytica Bd. I bewiesen. Er ist besonders bemerkenswert, weil er **nur** gilt, sobald n eine Primzahl ist. Denn ist n aus irgend zwei ungleichen Faktoren a und b zusammengesetzt, so werden diese Faktoren notwendig alle beide unter den Zahlen $1, 2, 3, \ldots n-1$ vorkommen, und die Gröfse $1 . 2 . 3 \ldots (n-1) + 1$ wird durch n geteilt den Rest $+1$ lassen. Dasselbe würde auch stattfinden, wenn n gleich dem Produkte zweier gleichen Faktoren $a \times a$ wäre; denn alsdann würden sich a und $2a$ in der Reihe $1, 2, 3 \ldots n-1$ vorfinden. Es würde somit das Produkt dieser Zahlen durch a^2 oder n teilbar sein, und das um 1 vermehrte Produkt würde den Rest 1 lassen.

Man kann hieraus eine **allgemeine** und untrügliche **Regel** ableiten, um zu erkennen, ob eine gegebene Zahl n **Primzahl** ist oder nicht. Dazu addiere man 1 zu dem Produkte

$$1 . 2 . 3 . 4 \ldots (n-1).$$

Ist die Summe durch n teilbar, so ist die Zahl n eine Primzahl; ist die Summe nicht durch n teilbar, so ist die Zahl n zusammengesetzt. Obwohl aber diese Regel theoretisch sehr schön ist, so hat sie doch in der Praxis wegen der ungeheuren Gröfse, zu welcher das Produkt $1 . 2 . 3 \ldots (n-1)$ bald anwächst, gar keinen Nutzen.

Wir bemerken, dafs die Zahlen $n-1$, $n-2$, $n-3$, ..., als Reste der Division durch n betrachtet, den Resten $-1, -2, -3, \ldots$ äquivalent sind; ferner ist, da n als ungerade Zahl vorausgesetzt wurde, die Anzahl der Faktoren $1, 2, 3, \ldots n-1$ eine gerade Zahl. Mithin wird das Produkt $1 . 2 . 3 \ldots (n-1)$ bei der Division durch n denselben Rest lassen, wie $\pm 1^2 \cdot 2^2 \cdot 3^2 \cdots \left(\frac{n-1}{2}\right)^2$, wobei das obere Zeichen gilt, wenn n von der Form $4k+1$, und das untere, wenn n von der Form $4k+3$ ist. Folglich:

1) Ist die Primzahl n von der Form $4k+1$, so ist die Gröfse $\left(1 \cdot 2 \cdot 3 \cdots \frac{n-1}{2}\right)^2 + 1$ durch n teilbar. Man kennt daher auf diese Weise von vornherein eine Summe von zwei Quadraten $a^2 + 1$, die durch n teilbar sein mufs.

2) Ist die Primzahl n von der Form $4k+3$, so ist die Gröfse $\left(1 \cdot 2 \cdot 3 \cdots \frac{n-1}{2}\right)^2 - 1$ durch n teilbar; mithin mufs n in einer der beiden Gröfsen

$$1 \cdot 2 \cdot 3 \cdots \frac{n-1}{2} + 1 \quad \text{oder} \quad 1 \cdot 2 \cdot 3 \cdots \frac{n-1}{2} - 1$$

aufgehen.

132.

Hülfssatz. Ist c eine Primzahl und P ein Polynom m^{ten} Grades, dessen Koefficienten ganze Zahlen sind, also

$$P = \alpha x^m + \beta x^{m-1} + \gamma x^{m-2} + \cdots + \omega,$$

so kann es zwischen $+\frac{1}{2}c$ und $-\frac{1}{2}c$ nicht mehr als m Werte von x geben, für welche dieses Polynom durch c teilbar ist.

Denn ist k ein erster Wert von x, für welchen P durch c teilbar ist, so kann man $P = (x-k)P' + Ac$ setzen und erhält für P' ein Polynom $m-1^{\text{ten}}$ Grades in x. Ist k' ein zweiter Wert von x, für welchen P durch c teilbar ist, so mufs für diesen Wert $(x-k)P'$ durch c teilbar sein. Nun kann aber der Faktor $x-k$, der in $k'-k$ übergeht, nicht durch c teilbar sein, da k und k' der Voraussetzung nach beide kleiner als $\frac{1}{2}c$ sind. Mithin kann P nur dann

zum zweiten Male durch c teilbar sein, wenn c ein Teiler von P' ist. Das Polynom P vom Grade m läfst somit nur eine Lösung mehr zu als das Polynom P' vom Grade $m-1$; es kann somit nicht mehr als m verschiedene Werte von x zwischen $+\frac{1}{2}c$ und $-\frac{1}{2}c$ geben, für welche P durch c teilbar ist.

Wir betrachten als **Lösung** oder **Wurzel** der Gleichung $\frac{P}{c}=e$ jeden **zwischen** $+\frac{1}{2}c$ und $-\frac{1}{2}c$ liegenden Wert von x, welcher die linke Seite zu einer ganzen Zahl macht. Die Anzahl dieser Lösungen, die man auch zwischen 0 und c nehmen könnte, darf niemals, wie eben bewiesen worden, den Exponenten m übersteigen. Hat man aber eine solche Lösung z. B. $x=k$, so kann man allgemeiner $x=k+cz$ setzen, wo z eine positive oder negative ganze Zahl bedeutet. Alsdann werden alle in dieser Formel enthaltenen Werte von x der Gleichung $\frac{P}{c}=e$ Genüge leisten.

133.

Satz. Ist c stets eine Primzahl und P ein Polynom m^{ten} Grades, welches ein Teiler ist von dem Binom $x^{c-1}-1$, so giebt es immer m Werte von x zwischen $+\frac{1}{2}c$ und $-\frac{1}{2}c$, für welche dieses Polynom durch c teilbar ist.

Es sei nämlich $x^{c-1}-1=PQ$, wo Q ein anderes Polynom vom Grade $c-1-m$ ist. Da es nun $c-1$ Werte von x giebt, für welche die linke Seite durch c teilbar wird, nämlich $\pm 1, \pm 2, \pm 3, \cdots \pm \frac{c-1}{2}$, so mufs für jeden dieser Werte entweder P oder Q durch c teilbar sein. Unter diesen $c-1$ Werten kann es nicht mehr wie m geben, für welche P durch c teilbar wird, da P nur vom Grade m ist; es kann aber auch nicht weniger als m geben, da sonst Q für mehr als $c-1-m$ Werte von x durch c teilbar sein müfste, was unmöglich ist, da Q nur vom Grade $c-1-m$ ist. Mithin ist die Anzahl der Werte von x, für welche P durch c teilbar ist und die zwischen $+\frac{1}{2}c$ und $-\frac{1}{2}c$ liegen, genau gleich m.

Bemerkung. Derselbe Satz würde gelten, wenn P ein Teiler von $x^{c-1}-1+cR$ wäre, wo R ein Polynom von beliebigem Grade darstellt.

134.

Satz. Ist die Primzahl c ein Teiler von $x^2 + N$, wo N eine gegebene positive oder negative Zahl bedeutet, so mufs die Gröfse $(-N)^{\frac{c-1}{2}} - 1$ durch c teilbar sein. Umgekehrt wird es, wenn diese Bedingung erfüllt ist, eine Zahl x (kleiner als $\frac{1}{2}c$) von der Beschaffenheit geben, dafs sich $x^2 + N$ durch c teilen läfst. (Ausgenommen wird der Fall $c = 2$, sowie der, wo N durch c teilbar ist).

1) Ist nämlich c ein Divisor von $x^2 + N$, so ergiebt sich, wenn man die Vielfachen von c aufser Acht läfst, $x^2 = -N$, folglich:

$$x^{c-1} - 1 = (-N)^{\frac{c-1}{2}} - 1.$$

Da nun die linke Seite durch c teilbar ist, so mufs es auch die rechte Seite sein.

2) Nimmt man an, dafs $(-N)^{\frac{c-1}{2}} - 1$ durch c teilbar sei, so setze man diese Gröfse gleich cr. Dies giebt:

$$x^{c-1} - 1 - cr = x^{c-1} - (-N)^{\frac{c-1}{2}}.$$

Setzt man aber für den Augenblick $c - 1 = 2b$, $-N = M$, so geht die rechte Seite über in $x^{2b} - M^b$, und dies ist teilbar durch $x^2 - M$ oder $x^2 + N$. Mithin geht $x^2 + N$ auch in der linken Seite

$$x^{c-1} - 1 - cr$$

auf. Es giebt daher (No. 133) notwendig zwei Werte von x, welche kleiner als $\frac{1}{2}c$ sind, und für welche $x^2 + N$ durch c teilbar wird. Diese beiden Werte sind im Grunde genommen nur einer, da sie sich nur durch ihr Vorzeichen von einander unterscheiden.

Bemerkung. Wir haben bewiesen, dafs, wenn N eine beliebige Zahl und c eine Primzahl ist, welche nicht in N aufgeht, die Gröfse $N^{c-1} - 1$ stets durch c teilbar ist. Diese Gröfse ist das Produkt der beiden Faktoren:

$$N^{\frac{c-1}{2}} + 1 \quad \text{und} \quad N^{\frac{c-1}{2}} - 1.$$

Es mufs daher entweder der eine oder der andere von diesen beiden Faktoren durch c teilbar sein. Daraus geht hervor, dafs die Gröfse $N^{\frac{c-1}{2}}$ bei der Division durch c jederzeit den Rest $+1$ oder den Rest -1 läfst.



135.

Da derartige Gröfsen wie $N^{\frac{c-1}{2}}$ sehr häufig im Verlaufe unserer Untersuchungen auftreten werden, so werden wir uns des **abgekürzten Zeichens**

$$\left(\frac{N}{c}\right)$$

bedienen, **um den Rest, welchen** $N^{\frac{c-1}{2}}$ **bei der Division durch** c **ergiebt, auszudrücken.** Dieser Rest kann, wie wir soeben gesehen haben, nur entweder gleich $+1$ oder gleich -1 sein.

Wenn $\left(\frac{N}{c}\right) = +1$ ist, so sagt man, N sei ein **quadratischer Rest** von c, weil alsdann $N^{\frac{c-1}{2}}$ bei der Division durch c den Rest $+1$ läfst, und dies die notwendige Bedingung dafür ist, dafs c in $x^2 - N$ aufgeht. Ist dagegen $\left(\frac{N}{c}\right) = -1$, so sagt man, N sei ein **quadratischer Nichtrest** von c.

In dem Ausdrucke $\left(\frac{N}{c}\right)$ bedeutet N eine beliebige positive oder negative Zahl, c dagegen immer eine Primzahl mit Ausnahme von 2.

Ist c eine Primzahl von der Form $4n+1$, so ist der Exponent $\frac{c-1}{2}$ eine gerade Zahl; dagegen ist dieser Exponent ungerade, sobald c eine Primzahl von der Form $4n+3$ ist. Im ersten Falle mufs somit

$$\left(\frac{-N}{c}\right) = \left(\frac{N}{c}\right),$$

im zweiten

$$\left(\frac{-N}{c}\right) = -\left(\frac{N}{c}\right)$$

sein.

Ein Ausdruck wie $\left(\frac{MN}{c}\right)$ ist stets das Produkt der beiden Ausdrücke $\left(\frac{M}{c}\right)$ und $\left(\frac{N}{c}\right)$. Denn setzt man:

$$\left(\frac{M}{c}\right) = \mu, \quad \left(\frac{N}{c}\right) = \nu,$$

so ist aus der Bedeutung dieser Ausdrücke ohne weiteres ersichtlich, dafs man

$$M^{\frac{c-1}{2}} = mc + \mu, \quad N^{\frac{c-1}{2}} = nc + \nu$$

setzen kann, wo m und n ganze Zahlen bedeuten. Daraus folgt:

$$(MN)^{\frac{c-1}{2}} = (mc + \mu)(nc + \nu).$$

Wie man sieht, läfst die rechte Seite bei der Division durch c den Rest $\mu\nu$; man erhält daher:

$$\left(\frac{MN}{c}\right) = \left(\frac{M}{c}\right)\left(\frac{N}{c}\right),$$

und ebenso für eine gröfsere Anzahl von Faktoren.

In dem Falle zweier gleichen Faktoren ist der Ausdruck $\left(\frac{MM}{c}\right)$, welcher dasselbe bedeutet wie $\left(\frac{M}{c}\right) \times \left(\frac{M}{c}\right)$ jederzeit gleich $+1$, da jeder Faktor $\left(\frac{M}{c}\right)$ nur entweder $+1$ oder -1 sein kann.

136.

Ist N eine gegebene Zahl und sucht man die Potenz N^x, für welche $N^x - 1$ durch die Primzahl c teilbar wird, so genügt es, wie man sieht, $x = c - 1$ zu setzen.

Will man ferner, dafs $N^x - 1$ durch die Potenz c^m der Primzahl c teilbar sei, so mufs man $x = c^{m-1}(c-1)$ setzen. Denn ist:

$$N^{c-1} - 1 = cM,$$

oder:

$$N^{c-1} = 1 + cM,$$

und erhebt man jede Seite auf die Potenz c^{m-1}, so erhält man:

$$N^x = (1 + cM)^{c^{m-1}}$$
$$= 1 + c^m M + \frac{c^{m-1} - 1}{2} c^{m+1} M^2 + \frac{(c^{m-1} - 1)(c^{m-2} - 2)}{1 \cdot 2 \cdot 3} c^{m+2} M^3 + \cdots$$

Hieraus sieht man, dafs, wenn man $x = (c-1)c^{m-1}$ setzt, die Gröfse $N^x - 1$ durch c^m teilbar ist.

Ist allgemein N eine gegebene Zahl und will man, dafs $N^x - 1$ durch eine andere Zahl A, welche prim zu N ist, teilbar sei, so mufs man A in seine Primfaktoren $a, b, c, \ldots$ zerlegen, so dafs

$$A = a^\alpha b^\beta c^\gamma \ldots$$

wird. Nimmt man dann:

$$x = a^{\alpha-1}(a-1)\, b^{\beta-1}(b-1)\, c^{\gamma-1}(c-1) \ldots,$$

so wird offenbar $N^x - 1$ zu gleicher Zeit durch a^α, b^β, c^γ, ... teilbar sein. Mithin ist diese Gröfse auch durch das Produkt

$$A = a^\alpha b^\beta c^\gamma \ldots$$

teilbar.

Da $a - 1$, $b - 1$, $c - 1$, ... einen oder mehrere gemeinsame Faktoren haben können, so erhält man, wenn man die kleinste Zahl, welche gleichzeitig durch $a - 1$, $b - 1$, $c - 1$, ... teilbar ist, A' nennt, einfacher:

$$x = A' a^{\alpha-1} b^{\beta-1} c^{\gamma-1} \ldots$$

137.

Hieraus erkennt man, dafs man eine Lösung jeder unbestimmten Gleichung ersten Grades

$$py - qz = r$$

unmittelbar erhalten kann. Dazu mufs man

$$y = rp^{x-1}$$

setzen und x derart bestimmen, dafs $p^x - 1$ durch die gegebene zu p relativ prime Zahl q teilbar sei. Denn nennt man h den Quotienten, so hat man:

$$z = \frac{r(p^x - 1)}{q} = rh.$$

Darauf ergiebt sich allgemeiner:

$$y = rp^{x-1} + qX$$
$$y = rh \quad + pX,$$

wo X eine beliebige positive oder negative Zahl ist. Man sieht aber auch, dafs diese Lösung meistens weit complicierter sein würde als die, welche man durch das gewöhnliche Kettenbruchverfahren erhält, welches nicht voraussetzt, dafs man zuvor die Primfaktoren der Zahl q gesucht habe. Siehe Bd. VIII der Nov. Com. Petrop. vom Jahre 1760 und 1761.

§ 2.

Untersuchung der Form, welche die Teiler der Formel $t^2 + au^2$ besitzen.

138.

In der Formel $t^2 + au^2$ betrachten wir a als eine gegebene positive oder negative Zahl und nehmen an, dafs t und u zwei unbestimmte Gröfsen sind, denen man alle nur möglichen ganzzahligen positiven oder negativen Werte beilegen kann, aber unter der wesentlichen Bedingung, dafs t und u **prim zu einander** sind. Denn ohne diese Bedingung würde jede Zahl ein Teiler der Formel $t^2 + au^2$ sein können, und es würde somit keine besondere Form geben, welche die Teiler der Formel $t^2 + au^2$ charakterisierte. Dies vorausgeschickt, erkennt man, dafs die Formel $t^2 + au^2$ für einen und denselben Wert von a unendlich viele verschiedene Zahlen darstellt, und es handelt sich darum, die **Beschaffenheit der Teiler** dieser Formel zu untersuchen.

Ist p ein beliebiger Teiler dieser Formel $t^2 + au^2$, und ist demzufolge:

$$t^2 + au^2 = Pp,$$

so behaupte ich zunächst, dafs die Zahlen u und p prim zu einander sind. Denn hätten u^2 und p einen gemeinschaftlichen Teiler ϑ, so würde offenbar ϑ auch ein Teiler von $Pp - au^2$ oder t^2 sein, und es würden somit t und u einen gemeinschaftlichen Teiler haben, was gegen unsere Voraussetzung ist. Da somit p und u prim zu einander sind, so kann man (No. 13) zwei Zahlen y und q von der Beschaffenheit finden, dafs

$$t = py + qu$$

ist. Substituiert man diesen Wert in die Gleichung $t^2 + au^2 = Pp$ und dividiert dann alles durch p, so erhält man:

$$py^2 + 2qyu + \frac{q^2 + a}{p} u^2 = P.$$

Da aber u mit p keinen Teiler gemeinsam hat, so kann diese Gleichung nur dann bestehen, wenn $\frac{q^2 + a}{p}$ eine ganze Zahl ist. Mithin wird die Zahl p, welche in der Formel $t^2 + au^2$ aufgeht, auch in der weniger allgemeinen Formel $x^2 + a$ aufgehen, wenn man $x = q$ setzt.

139.

Ebenso wie die zwei unbestimmte Gröfsen enthaltende Formel $t^2 + au^2$ keine andern Teiler wie die Formel mit einer einzigen Unbestimmten $t^2 + a$ oder $x^2 + a$ besitzt, so ist auch die Formel $At^2 + Btu + Cu^2$, in welcher A, B, C gegebene Zahlen sind, in dieser Beziehung nicht allgemeiner als die beiden ersten. Denn multipliciert man die letztere mit $4A$ und setzt man:

$$2At + Bu = x$$
$$4AC - B^2 = a,$$

so wird das Produkt:

$$x^2 + au^2.$$

Mithin sind die Teiler der Formel $At^2 + Btu + Cu^2$ dieselben wie die Teiler der einfacheren $x^2 + au^2$ oder noch einfacher wie die von $x^2 + a$, wobei a gleich der konstanten Gröfse $4AC - B^2$ ist. Und obwohl man die gegebene Formel mit $4A$ multipliciert hat, so machen doch sogar die Teiler, welche nicht prim zu A sind, keine Ausnahme, denn setzt man $x = B$, so geht die Formel $x^2 + a$ über in $B^2 + a$ oder $4AC$, dieselbe ist folglich teilbar durch A.

Ist stets p irgend ein Teiler der Formel $t^2 + au^2$, und nehmen wir an, dafs β, γ, δ, . . . die Primfaktoren von p seien, so mufs jede dieser Zahlen ein Teiler von $x^2 + a$ sein. Sonach müssen, der

Nr. 134 und der in Nr. 135 angegebenen Bezeichnung zufolge, die Gleichungen bestehen:

$$\left(\frac{-a}{\beta}\right) = 1, \quad \left(\frac{-a}{\gamma}\right) = 1, \quad \left(\frac{-a}{\delta}\right) = 1, \cdots$$

Diese Bedingungen sind auch hinreichend, wenigstens so lange p und a keinen gemeinschaftlichen Teiler haben.

140.

Kehren wir zu der Formel

$$py^2 + 2qyu + \frac{q^2 + a}{p} u^2 = P$$

zurück, und setzen wir, da $\frac{q^2 + a}{p}$ eine ganze Zahl ist,

$$\frac{q^2 + a}{p} = r,$$

so erhalten wir:

$$P = py^2 + 2qyu + ru^2.$$

Nun kann aber P ebenfalls als ein beliebiger Teiler der Formel $t^2 + au^2$ bezeichnet werden; mithin läfst sich jeder Teiler dieser unbestimmten Formel durch die Formel gleichen Grades

$$py^2 + 2qyu + ru^2$$

darstellen, in welcher $pr - q^2 = a$ ist.

Da man ferner $u = 1$ annehmen darf, weil die Formel $t^2 + a$ dieselben Teiler haben mufs, wie die Formel $t^2 + au^2$, so folgt daraus, dafs man auch einen beliebigen dieser Teiler durch die Formel $py^2 + 2qy + r$, in welcher gleichfalls $pr - q^2 = a$ ist, darstellen kann. Diese Form ist einfacher als die vorhergehende; indessen werden wir der letzteren den Vorzug geben, weil ihre Koefficienten immer zwischen bekannte und nur von der einen Zahl a abhängende Grenzen eingeschlossen werden können.

Wir haben nämlich (No. 54) bewiesen, dafs die unbestimmte Formel $py^2 + 2qyu + ru^2$ sich immer in eine andere ähnliche Formel transformieren läfst, bei welcher der mittlere Koefficient $2q$ keinen der beiden äufseren Koefficienten p und r übersteigt, und in der überdies stets $pr - q^2 = a$ ist.

Nehmen wir an, dafs diese Reduktion ausgeführt sei, so werden wir, je nachdem a positiv oder negativ ist, folgende Schlüsse zu ziehen berechtigt sein:

1) Jeder Teiler der Formel $t^2 + cu^2$, in welcher c eine positive Zahl ist, läfst sich darstellen durch die Formel

$py^2 + 2qyz + rz^2$, in welcher $pr - q^2 = c$, ferner $2q < p$ und $< r$ und demnach $q < \sqrt{\frac{c}{3}}$ ist.

2) Jeder Teiler der Formel $t^2 - cu^2$ läfst sich darstellen durch die Formel $py^2 + 2qyz - rz^2$, in welcher $pr + q^2 = c$, ferner $2q < p$ und $< r$ und demnach $q < \sqrt{\frac{c}{5}}$ ist.

141.

In beiden Fällen mufs man im Gedächtnis behalten, dafs die unbestimmten Gröfsen y und z relative Primzahlen sein müssen, wie es die unbestimmten Gröfsen t und u in der gegebenen Formel $t^2 \pm cu^2$ sind. Unter dieser Bedingung ist jede in der Formel $py^2 + 2qyz \pm rz^2$ enthaltene Zahl P notwendigerweise ein Teiler der Formel $t^2 \pm cu^2$.

Nimmt man nämlich an, dafs

$$P = p\alpha^2 + 2q\alpha\beta \pm r\beta^2$$

sei, und bedeutet $\frac{\alpha^0}{\beta^0}$ den Näherungsbruch, welcher in der Kettenbruchentwicklung von $\frac{\alpha}{\beta}$ letzterem Bruche vorhergeht, so erhält man, wenn man in der unbestimmten Formel $py^2 + 2qyz \pm rz^2$ an Stelle von y und z setzt: $\alpha y + \alpha^0 z$ und $\beta y + \beta^0 z$, nach No. 53 ein Resultat von der Form:

$$Py^2 + 2Qyz + Rz^2,$$

in welcher

$$PR = Q^2 \pm c$$

ist. Mithin ist P ein Teiler von $Q^2 \pm c$ oder von $t^2 \pm cu^2$.

§ 3.

Anwendung der vorhergehenden Theorie auf verschiedene Formeln wie:

$$t^2 + u^2, \quad t^2 + 2u^2, \quad t^2 - 2u^2, \ldots$$

Folgerungen, welche sich daraus in Bezug auf die allgemeinen Formen der Primzahlen ergeben.

142.

Um die Teiler der Formel

$$t^2 + u^2$$

zu erhalten, mufs man nach der Methode des vorigen Paragraphen setzen:



$$c = 1, \quad pr - q^2 = 1, \quad q < \sqrt{\tfrac{1}{3}}$$

Man erhält daher:

$$q = 0, \quad pr = 1, \quad p = r = 1,$$

und somit reduciert sich jeder Teiler $py^2 + 2qyz + rz^2$ auf $y^2 + z^2$. Folglich:

Jeder Teiler der Formel $t^2 + u^2$, welche aus zwei zu einander primen Quadraten besteht, ist gleichfalls die Summe zweier zu einander primen Quadrate.

Da dieser Satz in der Theorie der Zahlen sehr häufige Anwendung findet, so glauben wir noch einen zweiten auf andern Principien beruhenden Beweis für denselben geben zu müssen.

Ist N eine beliebige Zahl, welche in der Summe zweier zu einander primen Quadrate $t^2 + u^2$ aufgeht, so kann man annehmen, daſs die Zahlen t und u nicht gröſser seien als $\frac{1}{2}N$; denn da N ein Teiler ist von $t^2 + u^2$, so ist es auch ein Teiler von

$$(t - \alpha N)^2 + (u - \beta N)^2.$$

Diese Zahlen α und β kann man aber stets so wählen, daſs $t - \alpha N$ und $u - \beta N$ nicht gröſser sind als $\frac{1}{2}N$.

Wird diese Vorbereitung als ausgeführt vorausgesetzt, so ist die Gröſse $t^2 + u^2 < \frac{1}{2}N^2$; mithin erhält man, wenn man $t^2 + u^2 = NN'$ setzt, $N' < \frac{1}{2}N$.

Wäre nun zunächst $N' = 1$, so würde die Zahl N gleich $t^2 + u^2$ sein, und unsere Behauptung wäre richtig.

Es sei also $N' > 1$. Da nun N' ein Teiler von $t^2 + u^2$ ist, so ist es auch ein Teiler von

$$(t - \alpha N')^2 + (u - \beta N')^2.$$

Man kann aber α und β immer so wählen, daſs $t - \alpha N'$ und $u - \beta N'$ nicht gröſser sind als $\frac{1}{2}N$. Setzt man daher unter dieser Voraussetzung:

$$(t - \alpha N')^2 + (u - \beta N')^2 = N'N'',$$

so ist:

$$N'' < \frac{1}{2}N'.$$

Multipliciert man diese letzte Gleichung, Seite mit Seite, mit der Gleichung $t^2 + u^2 = NN'$, so findet man, daſs sich das Produkt auf die Form bringen läſst:

$$(t^2 + u^2 - \alpha t N' - \beta u N')^2 + (\alpha u N' - \beta t N')^2 = NN'^2N''.$$

Substituiert man auf der linken Seite NN' für $t^2 + u^2$ und dividiert dann durch N'^2, so wird:

$$(N - \alpha t - \beta u)^2 + (\alpha u - \beta t)^2 = NN''.$$

Wäre in diesem neuen Resultat $N'' = 1$, so würde die Zahl N gleich der Summe zweier Quadrate sein, und der Satz wäre bewiesen.

Ist aber noch $N'' > 1$, so leitet man auf demselben Wege aus dem Produkte NN'' ein neues Produkt NN''' ab, in welchem $N''' < \frac{1}{2} N''$ ist, und welches ebenfalls durch die Summe zweier Quadrate ausgedrückt ist.

Nun kann aber die Reihe der ganzen Zahlen $N, N', N'', N''', \ldots$, in welcher jedes Glied kleiner als die Hälfte des vorhergehenden ist, nicht ins Unendliche gehen; mithin gelangt man notwendigerweise zu einem Gliede, welches gleich 1 ist, und alsdann ist die Zahl N gleich der Summe zweier Quadrate.

143.

Wir kehren zur allgemeinen Methode zurück und stellen uns die Aufgabe, die Teiler der Formel

$$t^2 + 2u^2$$

zu suchen. In diesem Falle hat man:

$$c = 2, \quad pr - q^2 = 2, \quad q < \sqrt{\frac{2}{3}}.$$

Man muſs daher auch hier $q = 0$ setzen. Dies giebt:

$$pr = 2, \text{ und daher } p = 1, \quad r = 2.$$

Mithin ist der Teiler $py^2 + 2qyz + rz^2$ stets von der Form $y^2 + 2z^2$, also von derselben Form wie die zu teilende Formel $t^2 + 2u^2$.

Ist ferner die Formel

$$t^2 - 2u^2$$

gegeben, und sollen wir für diese einen beliebigen Teiler durch $py^2 + 2qyz - rz^2$ darstellen, so erhalten wir:

$$c = 2, \quad pr + q^2 = 2, \quad q < \sqrt{\frac{2}{5}}.$$

Daraus folgt $q = 0$ und $pr = 2$; demnach entweder $p = 1$, $r = 2$ oder $p = 2$, $r = 1$. Mithin kann jeder Teiler der Formel $t^2 - 2u^2$ entweder durch $y^2 - 2z^2$ oder durch $2y^2 - z^2$ dargestellt werden. Übrigens reducieren sich diese beiden Formen auf eine einzige; denn es ist, wie wir bereits bemerkt haben:



$$y^2 - 2z^2 = 2(y - z)^2 - (y - 2z)^2.$$

Ebenso findet man, dafs die Formel $t^2 + 3u^2$ als ungeraden Teiler nur eine Zahl von derselben Form $y^2 + 3z^2$ haben kann. Ferner kann die Formel $t^2 - 5u^2$ als ungeraden Teiler nur eine der beiden Formen $y^2 - 5z^2$ oder $5y^2 - z^2$ haben. Wie leicht zu sehen, reducieren sich aber diese beiden Formen ebenfalls auf eine einzige; denn es ist:

$$y^2 - 5z^2 = 5(y - 2z)^2 - (2y - 5z)^2.$$

Mithin allgemein:

Jede Zahl, welche in einer der Formen:

$$t^2 + u^2, \quad t^2 + 2u^2, \quad t^2 - 2u^2, \quad t^2 + 3u^2, \quad t^2 - 5u^2,$$

in denen t und u prim zu einander sind, enthalten ist, kann zu Teilern nur eine Zahl von derselben Form haben. Nur sind hinsichtlich der beiden letzten Formeln $t^2 + 3u^2$, $t^2 - 5u^2$ diejenigen Teiler, welche das Doppelte eines ungeraden sind, auszunehmen, da diese nicht von der Form $y^2 + 3z^2$ oder $y^2 - 5z^2$ sein können.

Diese verschiedenen Formen, welche den Vorteil bieten, dafs ihre Teiler von derselben Form sind, schliefsen sich gegenseitig nicht aus; im Gegenteil finden sich ziemlich häufig zwei oder mehrere in einer und derselben Zahl vereint. So ist z. B.

$$89 = 8^2 + 5^2 = 9^2 + 2 \cdot 2^2$$

$$241 = 15^2 + 4^2 = 13^2 + 2 \cdot 6^2 = 21^2 - 2 \cdot 10^2 = 7^2 + 3 \cdot 8^2 = 31^2 - 5 \cdot 12^2.$$

144.

Es dürfte hier am Orte sein, einige der Eigenschaften der Zahlen, welche auf der Verbindung von geraden und ungeraden Quadraten beruhen, zu entwickeln. Zunächst bemerken wir, dafs ein gerades Quadrat $(2x)^2$ stets von der Form $4n$, ein ungerades Quadrat $(2x + 1)^2$ von der Form $8n + 1$ ist. In der That ist:

$$4x^2 + 4x + 1 = 8\frac{x^2 + x}{2} + 1.$$

Nun ist aber $\frac{x^2 + x}{2}$ stets eine ganze Zahl, und ferner ist diese ganze Zahl eine Trigonalzahl.*)

*) Die verschiedenen Reihen von Zahlen, welche man figurierte Zahlen genannt hat, sind folgende:

Da somit y^2 und z^2 nur eine der Formen $4n$ oder $8n + 1$ besitzen können, so kann man unmittelbar die drei folgenden Sätze aufstellen.

1) Jede durch die Formel $y^2 + z^2$ dargestellte ungerade Zahl ist von der Form $4n + 1$.

2) Jede durch die Formel $y^2 + 2z^2$ dargestellte ungerade Zahl ist von einer der Formen $8n + 1$, $8n + 3$.

3) Jede durch die Formel $y^2 - 2z^2$ dargestellte ungerade Zahl ist von einer der Formen $8n + 1$, $8n + 7$.

A	$1, 2, 3, 4, 5, 6, \ldots n$
B	$1, 3, 6, 10, 15, 21, \ldots \frac{n(n+1)}{1 \cdot 2}$
C	$1, 4, 10, 20, 35, 56, \ldots \frac{n(n+1)(n+2)}{1 \cdot 2 \cdot 3}$
D	$1, 5, 15, 35, 70, 126, \ldots \frac{n(n+1)(n+2)(n+3)}{1 \cdot 2 \cdot 3 \cdot 4}$
u. s. w.	u. s. w.

Die erste Reihe A ist die der natürlichen Zahlen, deren allgemeines Glied n ist. Die zweite Reihe B ist die der Trigonalzahlen; ihr allgemeines Glied ist $\frac{n(n+1)}{2}$. Zieht man von diesem allgemeinen Gliede, welches das n^{te} Glied der Reihe B ist, das vorhergehende Glied derselben Reihe, welches $\frac{(n-1)n}{2}$ lautet, ab, so bleibt der Rest n, und dieser ist das allgemeine oder n^{te} Glied der Reihe A. Man bildet daher das n^{te} Glied der Reihe B, indem man das $n - 1^{\text{te}}$ Glied derselben Reihe zu dem n^{ten} Gliede der Reihe A addiert.

Die dritte Reihe C ist die der Pyramidalzahlen, deren allgemeines Glied $\frac{n(n+1)(n+2)}{1 \cdot 2 \cdot 3}$ ist. Zieht man von diesem Gliede das vorhergehende $\frac{(n-1)n(n+1)}{1 \cdot 2 \cdot 3}$ derselben Reihe ab, so bleibt die Differenz $\frac{n(n+1)}{1 \cdot 2}$, und diese ist das n^{te} Glied der Reihe B. Man kann also die Reihe C mit Hülfe der Reihe B ebenso bilden, wie man diese mit Hülfe der Reihe A gebildet hat.

Ebenso verhält es sich mit der vierten Reihe D, welches die Reihe der figurierten Zahlen dritter Ordnung ist und deren allgemeines Glied lautet: $\frac{n(n+1)(n+2)(n+3)}{1 \cdot 2 \cdot 3 \cdot 4}$. Analog ist es bei den andern.

Die allgemeinen Glieder, die wir hier als Definitionen gegeben haben und aus denen sich das Gesetz der successiven Bildung herleitet, schliefsen die ganze Theorie der figurierten Zahlen in sich und bieten unmittelbar den Beweis eines allgemeinen Satzes dar, den Fermat in seinen Anmerkungen zum Diophant S. 16 erwähnt und den er als eine seiner bedeutendsten Entdeckungen betrachtete. Anm. d. Verf.

Aus diesen drei Sätzen ergeben sich als Folgerungen die drei andern:

4) Eine Zahl von der Form $4n+3$ läfst sich nicht durch y^2+z^2 darstellen.

5) Eine Zahl von der Form $8n+5$ oder von der Form $8n+7$ läfst sich nicht durch y^2+2z^2 darstellen.

6) Eine Zahl von der Form $8n+3$ oder von der Form $8n+5$ läfst sich nicht durch y^2-2z^2 darstellen.

Nachdem dieses festgestellt ist, ist es leicht, die vier folgenden Sätze, welche in der Zahlentheorie von grofser Wichtigkeit sind, zu beweisen.

145.

1. Satz. Jede Primzahl von der Form $4n+1$ ist die Summe zweier Quadrate.

Ist diese Primzahl $c = 4n+1$, so ist:

$$x^{c-1} - 1 = x^{4n} - 1 = (x^{2n}+1)(x^{2n}-1).$$

Es giebt somit (No. 133) zwischen $+\frac{1}{2}c$ und $-\frac{1}{2}c$ $2n$ Werte von x, für welche $x^{2n}+1$ durch c teilbar ist. Nun ist aber $x^{2n}+1$ die Summe zweier zu einander primen Quadrate; mithin (No. 142) ist ihr Teiler c ebenfalls die Summe zweier zu einander primen Quadrate. Man kann daher immer $c = y^2+z^2$ setzen.*).

Bemerkung. Die Form $4n+1$ schliefst die beiden Formen $8n+1$ und $8n+5$ ein; mithin ist jede Primzahl von der Form $8n+1$ oder von der Form $8n+5$ die Summe zweier Quadrate.

146.

2. Satz. Jede Primzahl von der Form $8n+1$ besitzt zu gleicher Zeit die drei Formen: y^2+z^2, y^2+2z^2, y^2-2z^2.

Ist $c = 8n+1$ diese Primzahl, so mufs dieselbe, wie schon bewiesen, von der Form y^2+z^2 sein. Es bleibt mithin nur noch zu zeigen, dafs sie zu gleicher Zeit die beiden andern Formen y^2+2z^2 und y^2-2z^2 besitzt. Nun ist:

$$x^{c-1} - 1 = x^{8n} - 1 = (x^{4n}+1)(x^{4n}-1).$$

Mithin giebt es (No. 133) $4n$ zwischen $+\frac{1}{2}c$ und $-\frac{1}{2}c$ gelegene

*) Dieser Satz wurde oben (No. 52) auf eine noch direktere Weise bewiesen. Er ergiebt sich auch daraus, dafs, weil die Gleichung $x^2 - cy^2 = -$ in diesem Falle stets möglich ist (No. 43), c ein Teiler von x^2+1 sein mufs.
Anm. d. Verf.

Werte von x, für welche $x^{4n}+1$ durch c teilbar ist. Das Binom $x^{4n}+1$ kann man aber zunächst auf die Form $(x^{2n}-1)^2+2\cdot x^{2n}$ bringen, welche in der Formel t^2+2u^2 enthalten ist, wobei t und u relative Primzahlen sind. Folglich ist auch ihr Teiler c von der Form y^2+2z^2.

Ferner aber läſst sich das Binom $x^{4n}+1$ auch in der Form $(x^{2n}+1)^2-2x^{2n}$ schreiben, und diese stimmt mit t^2-2u^2 überein; folglich muſs sein Teiler c auch von der Form y^2-2z^2 sein.

Demnach besitzt jede Primzahl von der Form $8n+1$ zu gleicher Zeit die drei Formen: y^2+z^2, y^2+2z^2, y^2-2z^2. Ein Beispiel hierzu ist folgendes:

$$73=8^2+3^2=1^2+2\cdot 6^2=9^2-2\cdot 2^2.$$

147.

3. Satz. Jede Primzahl von der Form $8n+3$ ist von der Form y^2+2z^2.

Denn setzt man $c=8n+3$ und nimmt insbesondere $x=2$, so geht die Formel $x^{c-1}-1$ über in:

$$2^{8n+2}-1=(2^{4n+1}-1)(2^{4n+1}+1).$$

Demnach muſs der eine dieser binomischen Faktoren durch c teilbar sein. Wäre aber der erste Faktor, welcher von der Form $2t^2-u^2$ ist, durch c teilbar, so müſste die Zahl c selbst von der Form $2y^2-z^2$ oder y^2-2z^2 sein, die aber, wie wir in No. 144 gesehen haben, keiner Zahl von der Form $8n+3$ zukommt. Somit muſs c notwendig ein Teiler des zweiten Faktors $2\cdot 2^{4n}+1$ sein. Da dieser von der Form t^2+2u^2 ist, so muſs c von derselben Form y^2+2z^2 sein.*)

148.

4. Satz. Jede Primzahl von der Form $8n+7$ ist von der Form y^2-2z^2.

Denn setzt man $c=8n+7$ und nimmt ebenfalls $x=2$, so wird:

$$x^{c-1}-1=(2^{4n+3}+1)(2^{4n+3}-1).$$

Da die linke Seite (No. 129) durch c teilbar ist, so muſs auch einer der Faktoren der rechten Seite sich durch c teilen lassen. Verdoppelt man aber diese Faktoren und setzt $2^{2n+2}=k$, so werden dieselben zu k^2+2 und k^2-2. Wenn nun c in k^2+2 aufginge, so müſste c

*) Es ist oben (No. 44) bewiesen worden, daſs, wenn c eine Primzahl von der Form $8n+3$ ist, es immer möglich ist, der Gleichung $x^2-cy^2=-2$ zu genügen. Daraus folgt ganz direkt, daſs c ein Teiler von x^2+2 und somit c von der Form y^2+2z^2 ist. Anm. d. Verf.



von der Form $y^2 + 2z^2$ sein, die aber (No. 144) keiner Zahl $8n+7$ zukommen kann. Somit geht c notwendig in dem andern Faktor $k^2 - 2$ auf und es ist daher c von der Form $y^2 - 2z^2$.*)

149.

Allgemeiner Zusatz.

Aus diesen vier Sätzen ergiebt sich, daſs, wenn die ungeraden Primzahlen in vier Klassen oder Arten gemäſs den Formen

$$8n+1,\quad 8n+3,\quad 8n+5,\quad 8n+7$$

verteilt werden, man die folgenden Eigenschaften, durch welche je zwei Arten von den beiden andern unterschieden werden, feststellen kann:

1) Die Primzahlen von der Form $8n+1$ oder $8n+5$ sind allein, mit Ausschluſs aller andern, von der Form $y^2 + z^2$.

2) Die Primzahlen von der Form $8n+1$ oder $8n+3$ sind allein, mit Ausschluſs aller andern, von der Form $y^2 + 2z^2$.

3) Die Primzahlen von der Form $8n+1$ oder $8n+7$ sind allein, mit Ausschluſs aller andern, von der Form $y^2 - 2z^2$.

Man sieht hieraus, daſs nur die Gattung der Primzahlen von der Form $8n+1$, in welcher die Einheit enthalten ist, die drei Eigenschaften in sich vereinigt, und daſs jede der drei andern Arten nur eine einzige von diesen Eigenschaften besitzt.

Mit Hülfe dieser Sätze ist es leicht, den Wert des Ausdrucks $\left(\frac{2}{c}\right)$ für die verschiedenen Formen der Primzahl c zu finden. Man erinnere sich, daſs (No. 135) dieser Ausdruck den Rest bezeichnet, welchen $2^{\frac{c-1}{2}}$ bei der Division durch c übrig läſst, ein Rest, der nur entweder gleich $+1$ oder gleich -1 sein kann.

---

*) Auch dieses läſst sich unmittelbar mit Hülfe des Satzes in No. 45 beweisen; denn da diesem Satze zufolge die Gleichung $x^2 - cy^2 = 2$ stets möglich ist, so folgt daraus, daſs c in $x^2 - 2$ aufgeht und daher von der Form $y^2 - 2z^2$ ist.

Diese vier Sätze und einige andere ähnlicher Art sind von Fermat entdeckt worden; die Beweise dieses Gelehrten sind aber nicht auf uns gekommen. Euler hat den ersten und zweiten in den „Neuen Kommentarien" der Petersburger Akademie bewiesen; von den beiden andern hat Lagrange in den Abhandlungen der Berliner Akademie vom Jahre 1775 den Beweis geliefert.

Anm. d. Verf.

150.

5. Satz. Der Ausdruck $\left(\frac{2}{c}\right)$ ist gleich $+1$, wenn die Primzahl c von der Form $8n+1$ oder $8n+7$ ist; er ist gleich -1, wenn die Primzahl c die Form $8n+3$ oder die Form $8n+5$ besitzt.

1) Ist nämlich c von einer der Formen $8n+1$ oder $8n+7$, so kann man setzen:

$$c = y^2 - 2z^2,$$

oder:

$$2z^2 = y^2 - c.$$

Erhebt man beide Seiten auf die Potenz $\frac{c-1}{2}$ und läfst die Vielfachen von c aufser Acht, so erhält man:

$$2^{\frac{c-1}{2}} \cdot z^{c-1} = y^{c-1}.$$

Nach Weglassung derselben Vielfachen hat man aber auch (No. 129):

$$z^{c-1} = 1, \quad y^{c-1} = 1;$$

folglich:

$$2^{\frac{c-1}{2}} = 1,$$

oder nach unserer abgekürzten Bezeichnung:

$$\left(\frac{2}{c}\right) = 1.$$

2) Ist c von der Form $8n+3$, so kann man setzen:

$$c = y^2 + 2z^2$$

oder:

$$2z^2 = c - y^2.$$

Erhebt man beide Seiten auf die Potenz $\frac{c-1}{2}$ und beachtet man, dafs $\frac{c-1}{2}$ ungerade ist, so erhält man, indem man immer die Vielfachen von c fortläfst:

$$2^{\frac{c-1}{2}} z^{c-1} = -y^{c-1}$$

oder:

$$2^{\frac{c-1}{2}} = -1$$

oder endlich:

$$\left(\frac{2}{c}\right) = -1.$$

3) Ist c von der Form $8n+5$, so kann c nicht von der Form $y^2 - 2z^2$ sein; es kann daher auch nicht c in einer Zahl von der

Form $t^2 - 2u^2$ aufgehen. Wenn aber c in einer Zahl von dieser Form aufginge, so würde (zufolge No. 134) $\left(\frac{2}{c}\right) = 1$ sein. Da nun also nicht $\left(\frac{2}{c}\right) = 1$ sein kann, so mufs notwendig $\left(\frac{2}{c}\right) = -1$ sein.

Dieser Satz bildet in Verbindung mit den in No. 135 enthaltenen Bemerkungen eine Art von **Algorithmus,** der **für die Berechnung der Gröfsen** $\left(\frac{N}{c}\right)$ von grofsem Nutzen ist.

§ 4.
Beweis des Satzes, dafs jede ganze Zahl aus vier oder weniger Quadraten zusammengesetzt ist.

Wir beweisen zuerst den folgenden Satz, der nicht allein als blofser Hülfssatz dem in Aussicht genommenen Ziele dient, sondern auch eine sehr bemerkenswerte Eigenschaft der Primzahlen enthält.

151.

Satz. Ist eine Primzahl A und zwei beliebige andere Zahlen B und C, die positiv oder negativ, aber nicht durch A teilbar sein dürfen, gegeben, so kann man immer zwei Zahlen t und u von der Art finden, dafs die Gröfse $t^2 - Bu^2 - C$ durch A teilbar ist. (Lagrange, Abh. der Berl. Ak. 1770.)

1) Wenn man nämlich eine Zahl u von der Art finden kann, dafs $Bu^2 + C$ durch A teilbar ist, so nehme man für t ein Vielfaches von A. Alsdann wird die Formel $t^2 - Bu^2 - C$ durch A teilbar sein.

2) Wenn es keine Zahl giebt, welche diese Bedingung erfüllt, so setze man zur Abkürzung:

$$A = 2a + 1, \quad Bu^2 + C = V.$$

Da nun die in Rede stehende Gröfse $t^2 - Bu^2 - C$ oder $t^2 - V$ ein Teiler von $t^{2a} - V^a$ ist, so kann man den Quotienten

$$t^{2a-2} + Vt^{2a-4} + V^2 t^{2a-6} + \cdots + V^{a-1} = P$$

setzen, wodurch man erhält:

$$(t^2 - V)P = t^{2a} - V^a = t^{2a} - 1 - (V^a - 1).$$

Ist

$$Q = V^a + 1,$$

und multipliciert man beide Seiten mit Q, so ergiebt sich:

$$(t^2 - V)PQ = Q(t^{2a} - 1) - (V^{2a} - 1).$$

Nach dem Fermat'schen Satze (No. 129) weifs man aber, dafs die rechte Seite durch A teilbar ist, vorausgesetzt, dafs t und V prim

zu A sind. Wenn man also neben der Erfüllung der beiden Bedingungen noch bewirken kann, daſs weder P noch Q durch A teilbar ist, so kann man mit Sicherheit schlieſsen, daſs $t^2 - V$ durch A teilbar sei, und dies soll bewiesen werden.

Zunächst ist nun nach unserer Voraussetzung V niemals durch A teilbar; damit aber auch t durch A nicht teilbar sei, braucht man für t nur eine der Zahlen $1, 2, 3, \ldots A - 1$ zu nehmen. Auf diese Weise sind die beiden ersten Bedingungen von selbst erfüllt, und es bleibt nur noch übrig, den beiden andern Bedingungen zu genügen d. h. zu bewirken, daſs weder P noch Q durch A teilbar ist.

Nun giebt zuerst die Entwicklung der Gröſse

$$Q = V^a + 1 = (Bu^2 + C)^a + 1$$

die Gleichung:

$$\begin{aligned} Q = 1 + B^a u^{2a} &+ aB^{a-1}Cu^{2a-2} + \frac{a(a-1)}{1 \cdot 2} B^{a-2}C^2u^{2a-4} + \cdots \\ + C^a &+ aBC^{a-1}u^2 + \frac{a(a-1)}{1 \cdot 2} B^2C^{a-2}u^4 + \cdots \end{aligned}$$

Eins von beiden muſs nun stattfinden (No. 134): Entweder ist $C^a - 1$ teilbar durch A, oder $C^a + 1$ ist teilbar durch A. Findet der erste Fall statt, oder mit andern Worten, ist $\left(\frac{C}{A}\right) = 1$, so kann man $u = 0$ setzen, und die Gröſse Q wird nicht durch A teilbar sein. Dieser Fall ist übrigens an und für sich klar, da unabhängig von dem Gliede Bu^2, das man gleich Null oder gleich einem Vielfachen von A setzen kann, der Teil $t^2 - C$ durch A teilbar ist zufolge der Bedingung $\left(\frac{C}{A}\right) = 1$.

Findet aber der zweite Fall statt, oder ist $\left(\frac{C}{A}\right) = -1$, so erhält man, wenn man in Q den durch A teilbaren Teil $C^a + 1$ wegläſst und das Übrigbleibende durch u^2 dividiert, den Quotienten:

$$Q' = B^a u^{2a-2} + aB^{a-1}Cu^{2a-4} + \cdots + aBC^{a-1}.$$

Da diese Funktion in Bezug auf u betrachtet nur vom Grade $2a - 2$ oder $A - 3$ ist, so kann es höchstens $A - 3$ Werte von u geben, für welche Q' durch A teilbar ist. Mithin giebt es wenigstens zwei Werte von u, für welche Q' und somit auch Q nicht durch A teilbar ist.

Nachdem u auf diese Weise bestimmt ist, enthält zweitens die Funktion P nur noch die Veränderliche t, und da dieselbe in Bezug auf diese Veränderliche nur vom Grade $2a - 2$ oder $A - 3$ ist, so kann es zwischen 0 und A höchstens $A - 3$ Werte von t geben,

für welche P durch A teilbar ist. Mithin giebt es stets zwischen 0 und A wenigstens zwei Werte von t, für welche P nicht durch A teilbar ist.

Daher ist es stets möglich, den beiden verlangten Bedingungen zu genügen, so daſs die Gröſse $t^2 - Bu^2 - C$ durch die Primzahl A teilbar wird.

Zusatz. Setzt man $B = C = -1$, so folgt aus diesem Satze, daſs jede Primzahl A ein Teiler der Formel $t^2 + u^2 + 1$ ist. Dies hat Euler zuerst bewiesen im 5. Bde. der „Neuen Kommentarien der Petersburger Akademie".

152.

Hülfssatz. Das Produkt aus einer Summe von vier Quadraten in eine andere Summe von vier Quadraten ist ebenfalls wieder die Summe von vier Quadraten.

Um dies einzusehen, braucht man nur die folgende Formel, welche sich als eine identische erweist, zu entwickeln:

$$\begin{aligned}&(p^2 + q^2 + r^2 + s^2)(p'^2 + q'^2 + r'^2 + s'^2)\\ &= (pp' + qq' + rr' + ss')^2 + (pq' - qp' + rs' - sr')^2\\ &+ (pr' - qs' - rp' + sq')^2 + (ps' + qr' - rq' - sp')^2.\end{aligned}$$

In dieser Formel kann man nach Belieben das Vorzeichen jedes der darin vorkommenden Buchstaben ändern. Dadurch ergeben sich verschiedene Arten, das in Rede stehende Produkt in vier Quadrate zu zerlegen.*)

Bemerkung. Diesen schönen Satz der Algebra verdankt man ebenfalls Euler; derselbe ist später von Lagrange (Abh. der Berl. Akad. 1770) in folgender Weise verallgemeinert worden:

---

*) Man kann sich überzeugen, daſs eine ähnliche Formel nicht für drei Quadrate gilt, d. h. daſs das Produkt aus einer Summe von drei Quadraten in eine Summe von drei Quadraten nicht allgemein durch eine Summe von drei Quadraten ausgedrückt werden kann. Denn wäre dies möglich, so würde man das Produkt $(1 + 1 + 1)(16 + 4 + 1)$, welches gleich 63 ist, in drei Quadrate zerlegen können. Dies findet aber nicht statt, weder für die Zahl 63, noch für irgend eine Zahl von der Form $8n + 7$ (No. 155).

Ebenso oder mit Hülfe des Beispiels $(1 + 4 + 2 \cdot 4)(0 + 4 + 2 \cdot 1)$ würde man beweisen, daſs das Produkt zweier Formeln wie

$$p^2 + q^2 + 2r^2, \ p'^2 + q'^2 + 2r'^2$$

nicht allgemein gleich einer ähnlichen Formel $x^2 + y^2 + 2z^2$ sein kann.

Anm. d. Verf.



$$(p^2 - Bq^2 - Cr^2 + BCs^2)(p'^2 - Bq'^2 - Cr'^2 + BCs'^2)$$
$$= (pp' + Bqq' \pm Crr' \pm BCss')^2 - B(pq' + p'q \pm Crs' \pm Cr's)^2$$
$$- C(pr' - Bqs' \pm rp' \mp Bsq')^2 + BC(qr' - ps' \pm p's \mp rq')^2.$$

Man erkennt aus dieser Formel, dafs zwei Funktionen von der Form $x^2 - By^2 - Cz^2 + BCu^2$, wo B und C konstante Koefficienten sind, als Produkt eine ähnliche Funktion ergeben. Multipliciert man daher eine beliebige Anzahl derartiger Funktionen mit einander, so erhält man als Produkt eine Funktion derselben Art.

153.

Satz. Jede Primzahl A ist von der Form:

$$p^2 + q^2 + r^2 + s^2.$$

Wir haben in No. 151 gezeigt, dafs es stets zwei Zahlen t und u von der Art giebt, dafs $t^2 + u^2 + 1$ teilbar ist durch A. Setzt man aber $t - A\alpha$ und $u - A\beta$ an Stelle von t und u, so wird das Resultat $(t - A\alpha)^2 + (u - A\beta)^2 + 1$ ebenfalls durch A teilbar sein. Man kann daher annehmen, dafs die ursprünglichen Werte von t und u kleiner als $\frac{1}{2}A$ sind, oder dafs sie kleiner als $\frac{1}{2}A$ gemacht worden sind, indem man Vielfache von A davon abzog. Dies vorausgeschickt erhält man, wenn man

$$AA' = t^2 + u^2 + 1$$

setzt:

$$AA' < \frac{1}{4}A^2 + \frac{1}{4}A^2 + 1$$

oder:

$$A' < \frac{1}{2}A + \frac{1}{A}.$$

Betrachten wir allgemeiner die Gleichung:

$$AA' = p^2 + q^2 + r^2 + s^2,$$

in welcher jede der Zahlen p, q, r, s kleiner als $\frac{1}{2}A$ vorausgesetzt wird, so erhält man:

$$A'A < \frac{4}{4}A^2 \text{ oder } A' < A.$$

Hätte man nun zunächst $A' = 1$, so würde offenbar A gleich der Summe von vier Quadraten sein, und der Satz wäre bewiesen.

Es sei also $A' > 1$. Da A' ein Teiler von $p^2 + q^2 + r^2 + s^2$ ist, so wird es auch ein Teiler der Gröfse

$$(p - \alpha A')^2 + (q - \beta A')^2 + (r - \gamma A')^2 + (s - \delta A')^2$$

sein, wo die Zahlen α, β, γ, δ beliebig angenommen werden können. Nimmt man diese unbestimmten Zahlen derart an, dafs keins der



Glieder $p - \alpha A'$, $q - \beta A'$, $\cdots$ gröfser ist als $\frac{1}{2} A'$, und setzt man:

$$A'A'' = (p - \alpha A')^2 + (q - \beta A')^2 + (r - \gamma A')^2 + (s - \delta A')^2,$$

so erhält man:

$$A'A'' < \frac{4}{4} A'^2 \text{ oder } A'' < A'.$$

Multipliciert man nun mit Hülfe der Formel in No. 152 den Wert von AA' mit dem von $A'A''$, so findet man als Produkt eine Summe von vier Quadraten, deren jedes durch A'^2 teilbar ist. Dividiert man also das Ganze durch A'^2, so erhält man:

$$AA'' = (A - \alpha p - \beta q - \gamma r - \delta s)^2 + (\alpha q - \beta p + \gamma s - \delta r)^2 + (\alpha r - \gamma p + \delta q - \beta s)^2 + (\alpha s - \delta p + \beta r - \gamma q)^2.$$

Hat man nun $A'' = 1$, so ist der Satz bewiesen. Ist aber $A'' > 1$, so verfährt man in derselben Weise, um ein neues durch vier Quadrate ausgedrücktes Produkt AA''', in welchem $A''' < A''$ ist, zu erhalten. Setzt man so die Reihe der abnehmenden ganzen Zahlen $A, A', A'', A''', \ldots$ fort, so gelangt man notwendig zu einem Gliede, welches gleich 1 ist. Mithin ist aldann die Primzahl A ausgedrückt durch die Summe von vier Quadraten.

154.

Satz. Eine beliebige Zahl ist die Summe von vier oder weniger Quadraten.*)

Dies ist eine unmittelbare Folge des soeben bewiesenen Satzes und des vorhergenannten Hülfssatzes. Denn da eine beliebige Zahl das Produkt von mehreren gleichen oder ungleichen Primzahlen und jeder der Faktoren von der Form $p^2 + q^2 + r^2 + s^2$ ist, so ist klar, dafs, wenn man zwei Faktoren mit einander, sodann das Produkt der beiden mit einem dritten, ferner das Produkt der drei mit einem vierten Faktor u. s. w. multipliciert, bis alle Faktoren verbraucht sind, die aufeinanderfolgenden Produkte stets die Summe von vier Quadraten sind. Mithin wird auch das schliefsliche Produkt, welches die gegebene Zahl ist, die Summe von vier Quadraten sein und dargestellt werden können durch $p^2 + q^2 + r^2 + s^2$. Es steht dem übrigens nichts im Wege, dafs nicht eins oder mehrere der Quadrate p^2, q^2, r^2, s^2 gleich 0 sein könnten. Mithin ist jede beliebige Zahl gleich der Summe von vier oder weniger Quadraten.

*) Lagrange war der erste, der diesen schönen Satz bewies (Abh. der Berl. Akad. 1770). Später wurde dieser Beweis bedeutend vereinfacht von Euler in den Acta Petrop. vom Jahre 1777. Anm. d. Verf.

Wir bemerken an dieser Stelle, dafs eine Formel aus der Theorie der elliptischen Funktionen ein sehr einfaches und ganz direktes Mittel liefert zum Beweise desselben Satzes. Man findet nämlich in meinem Traité des fonctions elliptiques Bd. III Seite 133, dafs die Entwicklung der Potenz

$$(q^1 + q^9 + q^{25} + q^{49} + \cdots)^4$$

die Reihe liefert:

$$\frac{q^4}{1-q^8} + \frac{3q^{12}}{1-q^{24}} + \frac{5q^{20}}{1-q^{40}} + \frac{7q^{28}}{1-q^{56}} + \cdots$$

Daraus folgt unmittelbar, dafs jede Zahl von der Form $8n + 4$ die Summe von vier ungeraden Quadraten ist, woraus sich leicht schliefsen läfst, dafs jede beliebige Zahl die Summe von vier Quadraten ist. Die obige Identität kann ohne Zweifel durch rein analytische Betrachtungen bewiesen werden; man würde so den denkbar einfachsten Beweis unseres Satzes erhalten.

155.

Es giebt keine ganze Zahl, die nicht in der Formel

$$p^2 + q^2 + r^2 + s^2$$

enthalten wäre; zum gröfsten Teile lassen sie sich aber durch die einfachere Formel $p^2 + q^2 + r^2$ darstellen. Allgemein kann man behaupten, dafs jede ungerade Zahl, mit Ausnahme derer von der Form $8n + 7$, von der Form $p^2 + q^2 + r^2$ ist.

Die Zahlen von der Form $8n + 7$ bilden hiervon eine Ausnahme. Denn sind von den drei Gliedern p, q, r zwei gerade und das dritte ungerade, so ist die Formel $p^2 + q^2 + r^2$ von der Form $4n + 1$. Sind aber die drei Zahlen p, q, r ungerade, so ist die Formel $p^2 + q^2 + r^2$ von der Form $8n + 3$. Somit ist keine Zahl von der Form $8n + 7$ die Summe dreier Quadrate.

Nimmt man in der Formel $p^2 + q^2 + r^2 + s^2$ zwei Glieder als gleich an, so erhält man eine neue Formel $p^2 + q^2 + 2r^2$, die auch noch sehr allgemein ist, denn man kann behaupten, dafs jede ungerade Zahl ohne Ausnahme von der Form $p^2 + q^2 + 2r^2$ ist.

Diese Sätze werden später in noch helleres Licht gesetzt werden; gegenwärtig bemerken wir nur, dafs die beiden Formen $p^2 + q^2 + r^2$ und $p^2 + q^2 + 2r^2$, von denen in diesen Sätzen die Rede ist, in der Beziehung zu einander stehen, dafs das Doppelte der einen die andere hervorbringt. Man erkennt dies aus den Formeln:

$$2(p^2 + q^2 + r^2) = (p+q)^2 + (p-q)^2 + 2r^2$$
$$2(p^2 + q^2 + 2r^2) = (p+q)^2 + (p-q)^2 + (2r)^2.$$



156.

Der Satz, den wir in diesem Paragraphen bewiesen haben, bildet einen Teil einer von Fermat entdeckten allgemeinen Eigenschaft der Polygonalzahlen. Wir können nicht umhin, dieselbe anzuführen. Mit Rücksicht auf manche Leser müssen wir jedoch zunächst auseinandersetzen, was man unter Polygonalzahlen versteht.

Wenn man verschiedene arithmetische Reihen betrachtet, welche alle mit 1 beginnen, und deren konstante Differenzen der Reihe nach 1, 2, 3, 4, ... sind, und wenn man sodann durch Addition der Glieder jeder Reihe eine entsprechende Reihe bildet, so bilden diese verschiedenen Reihen diejenigen Zahlen, welche man Polygonalzahlen nennt. Dieselben sind in folgender Tafel enthalten:

Arithmetische Progressionen.	Reihe der Polygonalzahlen.
$1,\ 2,\ 3,\ 4,\ 5,\ \ldots n$	$1,\ 3,\ 6,\ 10,\ 15,\ \cdots \frac{n(n+1)}{2}$
$1,\ 3,\ 5,\ 7,\ 9,\ \ldots 2n-1$	$1,\ 4,\ 9,\ 16,\ 25,\ \ldots n^2$
$1,\ 4,\ 7,\ 10,\ 13,\ \ldots 3n-2$	$1,\ 5,\ 12,\ 22,\ 35,\ \cdots \frac{n(3n-1)}{2}$
$1,\ 5,\ 9,\ 13,\ 17,\ \ldots 4n-3$	$1,\ 6,\ 15,\ 28,\ 45,\ \cdots n(2n-1)$
. . . .	. . . .
$1,\ \alpha+1,\ 2\alpha+1\ \ldots n\alpha-\alpha+1$	$1,\ \alpha+2,\ 3\alpha+3\ \cdots \frac{n(n-1)}{2}\alpha+n.$

Die erste Reihe 1, 3, 6, ... ist die der Trigonalzahlen, die zweite 1, 4, 9, ... die der Quadratzahlen, die dritte 1, 5, 12, ... die der Pentagonalzahlen u. s. w.

Der soeben erwähnte Satz nun ist in der Fassung, welche Fermat demselben in seinen Anmerkungen zum Diophant Seite 180 gegeben hat, der folgende:

„Imo propositionem pulcherrimam et maxime generalem nos primi deteximus. Nempe omnem numerum vel esse triangulum vel ex duobus aut tribus triangulis compositum; esse quadratum vel ex duobus, tribus aut quatuor quadratis compositum; esse pentagonum vel ex duobus tribus quatuor aut quinque pentagonis compositum et sic deinceps in infinitum in hexagonis, heptagonis et polygonis quibuslibet, enuntianda videlicet pro numero angulorum generali et mirabili propositione. Ejus autem demonstrationem quae ex multis variis et

abstrusissimis numerorum mysteriis derivatur hic apponere non licet, opus enim et librum integrum huic operi destinare decrevimus et Arithmeticen hac in parte ultra veteres et notos terminos mirum in modum promovere."

[„Den folgenden sehr schönen und ganz allgemeinen Satz habe ich zuerst entdeckt: Jede Zahl ist entweder ein Dreieck (eine Trigonalzahl) oder aus zwei oder drei Dreiecken zusammengesetzt; sie ist entweder ein Quadrat oder aus zwei, drei oder vier Quadraten zusammengesetzt; sie ist ein Fünfeck oder aus zwei, drei, vier oder fünf Fünfecken zusammengesetzt, und so fort bei den Sechsecken, Siebenecken und beliebigen Vielecken bis ins Unendliche, indem sich immer der Ausspruch des allgemeinen und merkwürdigen Satzes nach der Anzahl der Winkel richtet. Den Beweis desselben, der sich auf viele verschiedene, sehr versteckte wunderbare Eigenschaften der Zahlen gründet, kann ich hier nicht beisetzen. Ich habe beschlossen, diesem Gegenstande ein ganzes Werk zu widmen und die Zahlenlehre in diesem Teile über die alten und bekannten Grenzen hinaus in staunenswerter Weise weiter zu entwickeln."]

Ich habe die eigenen Worte des Autors angeführt, weil man besonders aus dieser Stelle sieht, dafs sich Fermat mit einem grofsen Werke beschäftigte, welches, wie er selbst sagt, viele schöne Eigenschaften der Zahlen enthalten sollte. Die Mathematiker werden es noch lange bedauern, dafs dieser berühmte Gelehrte seine Absicht nicht verwirklicht hat oder wenigstens seine Verwandten und Freunde, welche seinen handschriftlichen Nachlafs erbten, nichts an die Öffentlichkeit haben gelangen lassen. Man würde darin aufser den noch unbekannten Beweisen mehrerer seiner Sätze ohne Zweifel Methoden finden, die dem Scharfsinn des Verfassers würdig wären, Methoden, die im Verein mit den späteren Entdeckungen viel dazu beigetragen haben würden, diesen sehr schwierigen Teil der exakten Wissenschaften zu vervollkommnen.

Beachtet man, um auf den erwähnten Satz zurückzukommen, dafs eine geringere Anzahl von Polygonalzahlen stets in einer gröfseren enthalten ist, da man an Stelle der fehlenden Glieder Null setzen kann, und Null in der That ein Glied jeder Reihe von Polygonalzahlen ist, so kann man den in Rede stehenden Satz kürzer in folgenden Worten aussprechen:

Jede beliebige Zahl kann durch Addition von drei Trigonalzahlen, ebenso durch Addition von vier Quadratzahlen, ferner durch Addition von fünf Pentagonalzahlen, von

sechs Hexagonalzahlen und so fort ins Unendliche gebildet werden.

157.

Ist also A eine gegebene Zahl, und sind $x, y, z, \ldots$ unbestimmte Zahlen, so kann man die verschiedenen Teile des allgemeinen Satzes in folgender Weise einzeln darstellen:

1) Welches auch die gegebene Zahl A sein möge, man kann stets der Gleichung

$$A = \frac{x^2 + x}{2} + \frac{y^2 + y}{2} + \frac{z^2 + z}{2}$$

oder, was auf dasselbe hinauskommt, der Gleichung

$$8A + 3 = (2x + 1)^2 + (2y + 1)^2 + (2z + 1)^2$$

Genüge leisten.

Wäre dieser erste Teil bewiesen, so würde er zeigen, daſs jede Zahl von der Form $8n + 3$ die Summe dreier Quadrate ist. Umgekehrt würde, wenn bewiesen wäre, daſs jede Zahl von der Form $8n + 3$ die Summe dreier Quadrate ist, unmittelbar daraus folgen, daſs jede ganze Zahl die Summe dreier Trigonalzahlen ist.

2) Welches auch die gegebene Zahl A sein möge, man kann stets der Gleichung

$$A = x^2 + y^2 + z^2 + u^2$$

Genüge leisten.

Dieser zweite Teil ist oben auf eine Art, die nichts zu wünschen übrig läſst, bewiesen worden. Es dürfte jedoch nicht unnützlich sein zu zeigen, daſs der erste Teil in notwendiger Verbindung mit dem zweiten steht. Wäre nämlich bewiesen, daſs man stets der Gleichung

$$8A + 3 = x^2 + y^2 + z^2$$

genügen kann, so würde daraus folgen:

$$8A + 4 = x^2 + y^2 + z^2 + 1.$$

Da aber die vier Quadrate der rechten Seite nur ungerade sein können, so sind die Zahlen $x + y$, $x - y$, $z + 1$, $z - 1$ gerade; mithin hat man in ganzen Zahlen:

$$4A + 2 = \left(\frac{x + y}{2}\right)^2 + \left(\frac{x - y}{2}\right)^2 + \left(\frac{z + 1}{2}\right)^2 + \left(\frac{z - 1}{2}\right)^2,$$

oder kürzer:

$$4A + 2 = x'^2 + y'^2 + z'^2 + u'^2.$$

Nun müssen aber von diesen vier Quadraten zwei gerade und zwei ungerade sein, da sonst ihre Summe nicht $4A + 2$ sein könnte.

Man erhält daher:

$$4A + 2 = 4a^2 + 4b^2 + (2c + 1)^2 + (2d + 1)^2,$$

und hieraus folgt:

$$2A + 1 = (a + b)^2 + (a - b)^2 + (c + d + 1)^2 + (c - d)^2.$$

Wird demnach der erste Teil des allgemeinen Satzes, welcher die Trigonalzahlen betrifft, als bewiesen vorausgesetzt, so ergiebt sich daraus als unmittelbare Folge, dafs jede ungerade Zahl $2A + 1$ die Summe von vier Quadraten ist. Ist aber eine Zahl die Summe von vier Quadraten $m^2 + n^2 + p^2 + q^2$, so ist das Doppelte derselben eine ähnliche Summe; denn es ist:

$$2(m^2 + n^2 + p^2 + q^2) = (m + n)^2 + (m - n)^2 + (p + q)^2 + (p - q)^2.$$

Folglich ist jede beliebige Zahl die Summe von vier Quadraten.

Man sieht, dafs der erste Teil des Fermat'schen Satzes implicite den zweiten einschliefst, und da der letztere auf anderm Wege vollkommen streng bewiesen ist, so kann man den ersten bereits mit einem grofsen Grade von Wahrscheinlichkeit als richtig ansehen.

3) Der dritte Teil des allgemeinen Satzes giebt:

$$A = \frac{3x^2 - x}{2} + \frac{3y^2 - y}{2} + \frac{3z^2 - z}{2} + \frac{3t^2 - t}{2} + \frac{3u^2 - u}{2}$$

oder:

$$24A + 5 = (6x - 1)^2 + (6y - 1)^2 + (6z - 1)^2 + (6t - 1)^2 + (6u - 1)^2,$$

so dafs dieser besondere Satz auf den folgenden zurückkommt:

Jede Zahl von der Form $24A + 5$ ist aus fünf Quadraten, deren Seiten von der Form $6m - 1$ sind, zusammengesetzt.

4) Der vierte Teil giebt:

$$A = x(2x-1) + y(2y-1) + z(2z-1) + s(2s-1) + t(2t-1) + u(2u-1)$$

oder:

$$8A + 6 = (4x - 1)^2 + (4y - 1)^2 + (4z - 1)^2 + (4s - 1)^2 + (4t - 1)^2 + (4u - 1)^2.$$

Also:

Jede Zahl von der Form $8A + 6$ mufs sich in sechs Quadrate zerlegen lassen, deren Seiten von der Form $4m - 1$ sind.

Überhaupt reduciert sich der in Rede stehende Satz immer auf die Zerlegung einer gegebenen Zahl in Quadrate, und alle besonderen Sätze sind in der folgenden allgemeinen Formel enthalten:

$$8\alpha A + (\alpha + 2)(\alpha - 2)^2 = (2\alpha x - \alpha + 2)^2 + (2\alpha y - \alpha + 2)^2 + \cdots$$

wobei die Anzahl der Glieder der rechten Seite $\alpha + 2$ ist.



§ 5.

Von der linearen Form, welche den Teilern der binomischen Formel $a^n \pm 1$, in der a und n gegebene Zahlen sind, zukommt.

158.

Die Betrachtung der Formel $a^n \pm b^n$, in welcher a und b zu einander prime Zahlen sind, würde keine gröſsere Allgemeinheit involvieren. Denn ist diese Formel durch die Primzahl p teilbar, so kann man immer $a = bx + py$ setzen, und es müſste $x^n \pm 1$ ebenfalls durch p teilbar sein. Dies vorausgeschickt, untersuchen wir nach einander die beiden Formeln $a^n + 1$ und $a^n - 1$.

Zunächst wollen wir die notwendige Bedingung dafür finden, daſs die Primzahl p ein Teiler der Formel $a^n + 1$ ist.

Welches auch p sein möge, man kann immer $p = 2nx + \pi$ annehmen, wo x eine unbestimmte Zahl und π eine positive Zahl kleiner als $2n$ ist. Man erhält daher, indem man die Vielfachen von p wegläſst,

$$a^n = -1.$$

Nach dem Fermat'schen Satze, und weil a nicht durch p teilbar sein kann, ist ferner:

$$a^{p-1} = +1$$

oder:

$$a^{2nx+\pi-1} = 1.$$

Wegen $a^n = -1$ hat man aber $a^{2nx} = 1$; mithin geht die vorige Gleichung über in:

$$a^{\pi-1} = 1,$$

so daſs wir die beiden Bedingungen

$$a^n = -1, \quad a^{\pi-1} = 1$$

zu befriedigen haben. Die zweite Bedingung ist von selbst erfüllt, wenn $\pi = 1$ ist; alsdann ist die Form des Teilers $p = 2nx + 1$.

Ist aber $\pi > 1$, so sei ω der gröſste gemeinschaftliche Teiler von n und $\pi - 1$. Dann kann man $n = n'\omega$ und $\pi - 1 = \pi'\omega$ setzen; dies giebt:

$$a^{n'\omega} = -1, \quad a^{\pi'\omega} = 1.$$

Da aber π' und n' prim zu einander sind, so kann man immer zwei ganze Zahlen f und g von der Beschaffenheit finden, daſs

$$fn' - g\pi' = 1$$

ist. Daraus folgt:

$$(-1)^f = a^{fn'\omega} = a^{g\pi'\omega + \omega} = a^{\omega},$$

oder:

$$a^{\omega} = (-1)^f.$$

Wird dieser Wert in die beiden Gleichungen $a^{n\omega} = -1$, $a^{\pi'\omega} = 1$ eingesetzt, so ergeben sich die beiden Bedingungen:

$$(-1)^{fn'} = -1, \qquad (-1)^{\pi' f} = 1.$$

Die erste zeigt, dafs f und n' ungerade Zahlen sein müssen; die zweite, dafs π' eine gerade Zahl ist. Letztere schliefst übrigens die erstere ein; denn ist π' gerade, so müssen, der Gleichung $fn' = g\pi' + 1$ zufolge, f und n' ungerade sein.

Nachdem dieses festgestellt ist, hat man:

$$a^{\omega} = -1,$$

d. h. $a^{\omega} + 1$ ist teilbar durch p.

Da nun die Annahmen $\pi = 1$ und $\pi > 1$ die beiden einzig möglichen sind, so kann man den folgenden allgemeinen Satz aufstellen:

159.

Jede Primzahl p, welche in der Formel $a^n + 1$ aufgeht, mufs entweder von der Form $2nx + 1$ oder wenigstens von der Form sein, welche für einen Teiler einer andern Formel $a^{\omega} + 1$, in welcher der Exponent ω gleich dem Quotienten aus n und einer ungeraden Zahl ist, notwendig ist.

Dieser Satz findet ebenso Anwendung auf die Teiler von $a^{\omega} + 1$ und läfst somit nach und nach alle Formen erkennen, welche die Teiler der gegebenen Formel $a^n + 1$ annehmen können. Einige der hauptsächlichsten Zusätze, die man unmittelbar daraus ableiten kann, und die auszusprechen genügt, sind folgende:

1) Ist der Exponent n eine ungerade Primzahl, so mufs jede Primzahl, welche in $a^n + 1$ aufgeht, von der Form $2nx + 1$ sein oder in $a + 1$ aufgehen.

2) Ist der Exponent n eine Potenz von 2, so kann die Formel $a^n + 1$ zu Teilern nur solche Primzahlen haben, welche in der Form $2nx + 1$ enthalten sind.

Sucht man z. B. die Primfactoren von

$$2^{32} + 1 = 4\,294\,967\,297,$$

so müssen dieselben in der Formel $64x + 1$ enthalten sein. Man probiere also nach einander die Zahlen 193, 257, 449, 577, 641. Die Division geht auf bei 641, und als Quotienten findet man 6700417. Um die Teiler dieses letzteren zu finden, mufs man gleichfalls mit



allen Primzahlen von der Form $64x + 1$, welche gröſser als 641 und kleiner als $2588 = \sqrt{6700417}$ sind, probieren. Es sind dies die folgenden:

$$769, \quad 1153, \quad 1217, \quad 1409, \quad 1601, \quad 2113.$$

Da keine dieser Zahlen in 6700417 aufgeht, so folgt daraus mit Sicherheit, daſs 6700417 eine Primzahl ist.

3) Ist $n = \lambda\nu$, wo λ ein Glied der Progression 2, 4, 8, 16, . . . und ν eine Primzahl ist, so ist jeder Primteiler der Formel $a^n + 1$ entweder von der Form $2nx + 1$ oder er ist ein Teiler der Formel $a^\lambda + 1$ und als solcher von der Form $2\lambda x + 1$.

4) Ist $n = \mu\nu$, wo μ und ν zwei ungerade Primzahlen sind, so ist der Primteiler der Formel $a^n + 1$ von der Form $2nx + 1$, oder er ist ein Teiler der Formel $a^\mu + 1$ und alsdann von der Form $2\mu x + 1$, oder er ist ein Teiler der Formel $a^\nu + 1$ und alsdann von der Form $2\nu x + 1$, oder endlich er ist ein Teiler von $a + 1$. Diese Fälle schlieſsen sich gegenseitig nicht aus; denn es ist z. B. jede Primzahl, welche in der Formel $a + 1$ aufgeht, offenbar auch ein Teiler aller andern Formeln $a^\nu + 1$, $a^\mu + 1$, u. s. w., und ebenso geht jede Primzahl, welche in $a^\nu + 1$ aufgeht, notwendigerweise auch in $a^n + 1$ auf.

160.

Es ist von keinem Nutzen, diese Zusätze auf eine gröſsere Anzahl von Fällen auszudehnen. Wir bemerken nur, daſs, wenn man die Teiler einer gegebenen Formel $a^n + 1$ finden soll, man nach und nach die Teiler aller andern Formeln $a^\omega + 1$, welche einen kleineren Exponenten haben, suchen muſs, indem man mit dem, in welchem der Exponent von a am kleinsten ist, beginnt. Man hat dann nur noch gemäſs der Form $2nx + 1$ die Teiler zu suchen, welche nicht durch die Formeln, die einen niedrigeren Exponenten haben als $a^n + 1$, gegeben werden.

Man beachte noch, daſs, wenn n eine ungerade Zahl ist, die Formel $a^n + 1$, mit a multipliciert, von der Form $x^2 + a$ wird, und daher zu Teilern nur die Primzahlen, welche in $x^2 + a$ aufgehen, haben kann. Diese Bedingung dient dazu, die Hälfte der in der Formel $2nx + 1$ enthaltenen Primzahlen auszuschlieſsen; jedoch muſs man zu diesem Zwecke das beachten, was wir weiter unten von den Teilern von $x^2 + a$ beweisen werden. Für jetzt sieht man, daſs, wenn a gleich 2 wäre, die Teiler von $x^2 + 2$ nur von den

Formen $8m + 1$, $8m + 3$ sein können. Daher kommt es, daſs die beiden andern allgemeinen Formen $8m + 5$, $8m + 7$ ausgeschlossen und niemals Teiler der Formel $2^n + 1$ sind, wenn n ungerade ist. Eine ähnliche Ausschlieſsung findet bei andern Werten von a ebenfalls statt.

161.

Beispiel.

Wir stellen uns die Aufgabe, alle Teiler der Zahl

$$549755813889 = 2^{39} + 1 = A$$

zu finden.

Wir betrachten zuerst die Formeln mit niedrigerem Exponenten

$$2^{13} + 1, \quad 2^3 + 1, \quad 2^1 + 1.$$

Die letzte ergiebt 3 als Teiler aller vorhergehenden Formeln.

Die Formel $2^3 + 1 = 9$ giebt ebenfalls nur 3 als Primteiler; sie lehrt aber ferner, daſs A durch 9 teilbar ist.

Die Formel $2^{13} + 1 = 8193 = 3 \,.\, 2731$ kann, wenn sie einen andern Teiler als 3 hat, nur einen solchen von der Form $26x + 1$ haben. Da aber die kleinste in der Form $26x + 1$ enthaltene Primzahl 53 bereits zu groſs ist, da sie die Quadratwurzel aus 2731 übersteigt, so folgt daraus, daſs 2731 eine Primzahl ist, und daſs somit $2^{13} + 1$ keinen andern Teiler hat als 3 und 2731.

Hiernach muſs die Zahl A teilbar sein durch $9 \,.\, 2731$. Dividiert man sie zuerst durch $3 \,.\, 2731$, welche Zahl gleich $2^{13} + 1$ ist, so ist der Quotient $2^{26} - 2^{13} + 1 = 67100673$, und dividiert man diese durch 3, so erhält man $A = 3^2 \,.\, 2731 \,.\, 22\,366\,891$.

Man hat daher nur noch die Teiler der Zahl

$$B = 22\,366\,891$$

zu suchen. Diese Teiler müssen von der Form $78x + 1$ sein, und da sie auch in der Formel $t^2 + 2$ aufgehen müssen, so können sie nur die Formen $8n + 1$, $8n + 3$ haben. Die Form $78x + 1$ enthält aber vier andere, je nachdem x gleich einer der Zahlen

$$4y, \quad 4y + 1, \quad 4y + 2, \quad 4y + 3$$

ist. Diese vier Formen sind:

$$312y + 1, \quad 312y + 79, \quad 312y + 157, \quad 312y + 235.$$

Die zweite und die dritte müssen ausgeschlossen werden, da sie von der Form $8n + 7$ und $8n + 5$ sind. Mithin ist jede Primzahl, welche in B aufgeht, in einer der beiden Formen enthalten:

$$312y + 1, \quad 312y + 235.$$

Die Primzahlen, welche in diesen Formen enthalten und zugleich kleiner sind als $\sqrt{B}$, welches ungefähr 4620 ist, sind folgende:

313, 547, 859, 937, 1171, 1249, 1483, 1873, 2731,
3121, 3433, 4057, 4603.

Probiert man der Reihe nach mit diesen dreizehn Zahlen oder nur mit zwölf (denn es ist überflüssig mit 2731 zu probieren), so findet man, daſs keine von ihnen in B aufgeht. Daraus folgt, daſs 22 366 891 eine Primzahl ist.

Da die Zahl B ein Teiler von $t^2 + 2$ ist, so muſs sie von der Form $p^2 + 2q^2$ sein. Will man B wirklich auf diese Form bringen, so kann dies ohne Probieren mit Hülfe der folgenden Formel geschehen:

$$\frac{4m^4 - 2m^2 + 1}{3} = \left(\frac{2m^2 \pm 2m - 1}{3}\right)^2 + 2\left(\frac{2m^2 \mp m - 1}{3}\right)^2.$$

Nun ist $B = \frac{2^{26} - 2^{13} + 1}{3}$; setzt man also $m = 2^6$, so findet man:

$$B = (2773)^2 + 2(2709)^2.$$

162.

Wir gehen jetzt zur zweiten Frage über und stellen uns die Aufgabe, die Form, welche die Primteiler der gegebenen Zahl $a^n - 1$ haben müssen, zu finden.

Wie beschaffen die Primzahl p, welche in dieser Formel aufgeht, auch sein möge, man kann sie immer von der Form $p = nx + \pi$ annehmen, wo π eine positive Zahl kleiner als n ist. Man erhält daher, wenn die Vielfachen von p weggelassen werden:

$$a^n = 1 \quad \text{und} \quad a^{p-1} = 1,$$

und daraus folgt:

$$a^{\pi - 1} = 1.$$

In dieser letzteren Gleichung kann man nur $\pi = 1$ oder $\pi > 1$ annehmen.

1) Ist $\pi = 1$, so ist die Form des Teilers $p = nx + 1$. Sie bleibt so, so lange n gerade ist; ist aber n ungerade, so muſs notwendig x gerade sein, und daher hat man $p = 2nz + 1$.

2) Ist $\pi > 1$, und ist ω der gröſste gemeinschaftliche Teiler von n und $\pi - 1$, (wo ω gleich 1 sein muſs, wenn es kein anderes gemeinsames Maſs giebt), so kann man immer zwei ganze Zahlen f und g von der Beschaffenheit finden, daſs

$$fn - g(\pi - 1) = \omega$$

ist. Nun ergeben die beiden Gleichungen $a^n = 1$, $a^{\pi-1} = 1$ die folgenden:

$$1 = a^{fn} = a^{g(\pi-1)+\omega} = a^{\omega},$$

oder:

$$a^{\omega} = 1.$$

Mithin ist p ein Teiler von $a^{\omega} - 1$. Hierbei ist dem Resultate $a^{\omega} = 1$ keine Einschränkung hinzuzufügen, weil die Gleichung $a^{\omega} = 1$ den beiden Gleichungen $a^n = 1$ und $a^{\pi-1} = 1$ genügt.

Hiernach ist die ganze Theorie der Teiler von $a^n - 1$ in dem folgenden Satze enthalten:

163.

Jede Primzahl p, welche in der Formel $a^n - 1$ aufgeht, mufs entweder in der Form $p = nx + 1$ enthalten oder auch ein Teiler der Formel $a^{\omega} - 1$ sein, in welcher ω ein Teiler von n ist.

Wir fügen hinzu, dafs, wenn n ungerade ist, in welchem Falle die Form $nx + 1$ in $2nz + 1$ übergeht, der Teiler p auch in denjenigen Formen enthalten sein mufs, welche den Teilern der Formel $x^2 - a$ zukommen.

Derselbe Satz findet Anwendung auf die Formel $a^{\omega} - 1$ oder auf jede andere, welche unmittelbar aus den Teilern von n sich ergiebt. Daher erhält man durch Vereinigung der Resultate alle Teiler der gegebenen Formel. Einige allgemeine Zusätze, welche sich daraus ergeben, sind folgende:

1) Ist die Zahl n eine Primzahl, so sind die Teiler der Formel $a^n - 1$ in der Form $2nz + 1$ enthalten, mit alleiniger Ausnahme derer, welche in $a - 1$ aufgehen.

2) Wenn die Zahl n das Produkt zweier Primzahlen μ und ν (2 ausgenommen) ist, so wird der Primteiler p der Formel $a^n - 1$ entweder von der Form $2nz + 1$ sein, oder er ist ein Teiler von $a^{\mu} - 1$ und alsdann von der Form $2\mu z + 1$, oder er ist ein Teiler von $a^{\nu} - 1$ und alsdann von der Form $2\nu z + 1$, oder endlich er ist ein Teiler von $a - 1$ und von der Form $2z + 1$, welche allen Primzahlen zukommt. Denn ist n eine ungerade Zahl, so geht offenbar $a - 1$ in $a^n - 1$ auf; mithin mufs jeder Teiler der ersten Gröfse auch ein Teiler der zweiten sein.

3) Ist die Zahl n eine Potenz von 2, und setzt man $\alpha = \frac{1}{2}n$, $\beta = \frac{1}{2}\alpha$, $\gamma = \frac{1}{2}\beta, \cdots$, so ist der Teiler p der Formel

$a^n - 1$ entweder von der Form $nx + 1$, oder er ist von der Form $\alpha x + 1$ und ein Teiler von $a^\alpha - 1$, oder er ist von der Form $\beta x + 1$ und ein Teiler der Formel $a^\beta - 1$, und so fort bis zur Form $2x + 1$, welche in $a^2 - 1$ aufgeht.

164.

Beispiel 1.

Um sämtliche Teiler der Zahl $A = 2^{32} - 1$ zu erhalten, bilden wir die folgende Tafel, in welcher man die gegebene Formel und die daraus sich ergebenden Formeln nebst den entsprechenden Formen des Teilers sieht:

$$\begin{array}{ll} p = 32x + 1, & A = 2^{32} - 1 = (2^{16} + 1)B \\ p = 16x + 1, & B = 2^{16} - 1 = (2^8 + 1)C \\ p = 8x + 1, & C = 2^8 - 1 = (2^4 + 1)D \\ p = 4x + 1, & D = 2^4 - 1 = (2^2 + 1)E \\ p = 2x + 1, & E = 2^2 - 1 = 3. \end{array}$$

Die letzte Zahl E, welche sich auf 3 reduciert, mufs alle vorhergehenden teilen; und zwar hat man:

$$D = (2^2 + 1)3 = 3 \cdot 5$$
$$C = (2^4 + 1)D = 3 \cdot 5 \cdot 17.$$

Die Zahl B enthält dieselben Teiler wie C und aufserdem noch $2^8 + 1 = 257$, welches eine Primzahl ist. Endlich ist A das Produkt aus B und $2^{16} + 1 = 65537$. Da nun $2^{16} + 1$ mit $2^{16} - 1$ keinen gemeinschaftlichen Teiler haben kann, so folgt, dafs die Teiler von $2^{16} + 1$ oder 65537 nur Primzahlen von der Form $32x + 1$ sein können. Die Primzahlen aber, welche in dieser Form enthalten und kleiner als $\sqrt{65537}$ sind, sind 97 und 193, und diese gehen nicht in 65537 auf. Demnach ist 65537 eine Primzahl, und die Zahl A, in ihre Primfaktoren zerlegt, ist:

$$A = 3 \cdot 5 \cdot 17 \,.\, 257 \cdot 65537.$$

Multipliciert man diesen Wert mit demjenigen, den wir (S. 15) für $2^{32} + 1$ gefunden hatten, so erhält man den in Faktoren zerlegten Wert von $2^{64} - 1$.

165.

Beispiel 2.

Es sei ferner die Zahl $A = 2^{31} - 1$ gegeben. Da der Exponent 31 eine Primzahl ist, so können die Teiler von A nur von der Form

$62x + 1$ sein, und zwar giebt es hiervon keine Ausnahme, da sich $a - 1$ in diesem Falle auf $2 - 1 = 1$ reduciert. Beachtet man zugleich, dafs die Zahl $2A$ von der Form $t^2 - 2$ ist, und dafs somit die Teiler von A von einer der Formen $8n + 1$, $8n + 7$ sein müssen, so findet man, indem man diese letzteren Formen mit der ersten $62x + 1$ kombiniert, dafs jeder Primteiler von A notwendig von einer der Formen $248z + 1$, $248z + 63$ ist. Nun zeigt aber Euler (Abhandl. der Berl. Akad. 1772 S. 36), dafs man, nachdem man alle in diesen Formen enthaltenen Primzahlen bis zu 46339, der Quadratwurzel der Zahl A, probiert hat, keine findet, welche in A aufgeht. Daraus folgt, in Übereinstimmung mit einer Behauptung Fermat's, dafs die Zahl $2^{31} - 1 = 2\,147\,483\,647$ eine Primzahl ist. Dies ist die gröfste von allen Primzahlen, welche bis heute als solche bestätigt sind.

Wir wollen diesen Paragraphen nicht ohne die Bemerkung beschliefsen, dafs Euler der Urheber der hauptsächlichsten, in ihm enthaltenen Sätze ist. Siehe den 1. Bd. der Novi Comment. Petrop.

§ 6.

Satz, enthaltend ein Reciprocitätsgesetz, welches zwischen zwei beliebigen Primzahlen besteht.

166.

Wir haben in No. 135 gesehen, dafs, wenn m und n irgend zwei ungerade und ungleiche Primzahlen sind, die abgekürzten Ausdrücke $\left(\frac{m}{n}\right)$ und $\left(\frac{n}{m}\right)$ der erstere den Rest, welcher bei der Division von $m^{\frac{n-1}{2}}$ durch n bleibt, der andere den Rest, welcher bei der Division von $n^{\frac{m-1}{2}}$ durch m bleibt, darstellen. Gleichzeitig haben wir bewiesen, dafs diese beiden Reste stets nur entweder $+1$ oder -1 sein können. Dies vorausgeschickt, existiert zwischen den beiden Resten $\left(\frac{m}{n}\right)$ und $\left(\frac{n}{m}\right)$ **eine Relation** von der Beschaffenheit, dafs, wenn der eine bekannt ist, auch der andere unmittelbar bestimmt ist. Der allgemeine Satz, welcher diese Beziehung enthält, ist folgender:

Welches auch die Primzahlen m und n sein mögen, man

erhält stets, falls sie nicht alle beide von der Form $4x + 3$ sind:

$$\left(\frac{n}{m}\right) = \left(\frac{m}{n}\right).$$

Sind sie aber alle beide von der Form $4x + 3$, so hat man:

$$\left(\frac{n}{m}\right) = -\left(\frac{m}{n}\right).$$

Diese beiden allgemeinen Fälle sind in die Formel zusammengefafst:

$$\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}\cdot\left(\frac{m}{n}\right).$$

Um die verschiedenen Fälle dieses Satzes zu entwickeln, ist es erforderlich, durch besondere Buchstaben die Primzahlen von der Form $4x + 1$ von denen von der Form $4x + 3$ zu unterscheiden. Wir werden im Verlaufe dieses Beweises die ersteren mit den Buchstaben A, a, α, die letzteren mit den Buchstaben B, b, β bezeichnen. Alsdann schliefst der soeben ausgesprochene Satz die folgenden acht Fälle ein:

I. Ist $\left(\frac{a}{b}\right) = -1$, so folgt: $\left(\frac{b}{a}\right) = -1$.

II. Ist $\left(\frac{b}{a}\right) = +1$, so folgt: $\left(\frac{a}{b}\right) = +1$.

III. Ist $\left(\frac{B}{b}\right) = +1$, so folgt: $\left(\frac{b}{B}\right) = -1$.

IV. Ist $\left(\frac{B}{b}\right) = -1$, so folgt: $\left(\frac{b}{B}\right) = +1$.

V. Ist $\left(\frac{a}{A}\right) = +1$, so folgt: $\left(\frac{A}{a}\right) = +1$.

VI. Ist $\left(\frac{a}{A}\right) = -1$, so folgt: $\left(\frac{A}{a}\right) = -1$.

VII. Ist $\left(\frac{a}{b}\right) = +1$, so folgt: $\left(\frac{b}{a}\right) = +1$.

VIII. Ist $\left(\frac{b}{a}\right) = -1$, so folgt: $\left(\frac{a}{b}\right) = -1$.

167.

Beweis der Fälle I und II.

Ich bemerke zunächst, dafs die Gleichung

$$x^2 + ay^2 = bz^2$$

oder allgemeiner

$$(4f + 1)x^2 + (4g + 1)y^2 = (4n + 3)z^2$$

unmöglich ist. Denn da x und y als relative Primzahlen vorausgesetzt sind, so ist die linke Seite stets in den Formen $4k+1$ und $4k+2$ enthalten, während die rechte Seite nur von einer der Formen $4k$ und $4k+3$ sein kann.

Nach No. 27 würde aber die Gleichung $x^2 + ay^2 = bz^2$ lösbar sein, wenn man zwei ganze Zahlen λ und μ von der Beschaffenheit finden könnte, dafs $\frac{\lambda^2 + a}{b}$ und $\frac{\mu^2 - b}{a}$ ganze Zahlen würden. Andrerseits ist die Bedingung dafür, dafs b ein Teiler von $\lambda^2 + a$ sei, die folgende:

$$\left(\frac{-a}{b}\right) = 1 \quad \text{oder} \quad \left(\frac{a}{b}\right) = -1,$$

und ebenso ist die Bedingung dafür, dafs a ein Teiler von $\mu^2 - b$ sei:

$$\left(\frac{b}{a}\right) = +1.$$

Mithin könnte man nicht gleichzeitig haben:

$$\left(\frac{a}{b}\right) = -1 \quad \text{und} \quad \left(\frac{b}{a}\right) = +1.$$

Ferner kann aber jeder dieser Ausdrücke nur $+1$ oder -1 sein. Folglich:

I. Ist $\left(\frac{a}{b}\right) = -1$, so ergiebt sich $\left(\frac{b}{a}\right) = -1$.

II. Ist $\left(\frac{b}{a}\right) = +1$, so ergiebt sich $\left(\frac{a}{b}\right) = +1$.

Übrigens sind diese beiden Sätze derart unter einander verbunden, dafs der eine nur eine Folge des andern ist. Denn nimmt man den ersten als richtig an, und ist $\left(\frac{b}{a}\right) = +1$, so könnte nicht $\left(\frac{a}{b}\right) = -1$ sein, da sich sonst gegen die Annahme $\left(\frac{b}{a}\right) = -1$ ergeben würde. Man erhält daher $\left(\frac{a}{b}\right) = +1$.

168.

Beweis der Fälle III und IV.

Sind B und b zwei Primzahlen von der Form $4n+3$, so ist es, wie wir in No. 47 bewiesen haben, immer möglich, einer der beiden Gleichungen

$$Bx^2 - by^2 = +1, \qquad Bx^2 - by^2 = -1$$

Genüge zu leisten.

1) Ist $\left(\frac{B}{b}\right) = +1$, so kann die Gleichung $Bx^2 - by^2 = -1$

nicht stattfinden; denn wäre sie erfüllt, so würde b ein Teiler von Bx^2+1 oder von z^2+B sein. Darnach müfste man haben: $\left(\frac{-B}{b}\right)=1$ oder $\left(\frac{B}{b}\right)=-1$, entgegen der Voraussetzung. Nachdem so die eine der beiden Gleichungen ausgeschlossen ist, mufs die andere notwendig stattfinden. Aus dieser erkennt man aber, dafs B ein Teiler von by^2+1 oder von z^2+b ist. Mithin hat man $\left(\frac{-b}{B}\right)=1$ oder $\left(\frac{b}{B}\right)=-1$.

2) Ist $\left(\frac{B}{b}\right)=-1$, so beweist man analog, dafs die Gleichung $Bx^2-by^2=+1$ unmöglich ist. Mithin findet notwendig die andere Gleichung $Bx^2-by^2=-1$ statt. Folglich ist B Teiler von by^2-1 oder von z^2-b, und dies giebt: $\left(\frac{b}{B}\right)=+1$. Also:

III. Ist $\left(\frac{B}{b}\right)=+1$, so ergiebt sich $\left(\frac{b}{B}\right)=-1$.

IV. Ist $\left(\frac{B}{b}\right)=-1$, so ergiebt sich $\left(\frac{b}{B}\right)=+1$.

Man ersieht hieraus, dafs $\left(\frac{B}{b}\right)$ und $\left(\frac{b}{B}\right)$ immer von entgegengesetztem Zeichen sind.

169.

Beweis der Fälle V und VI.

Ist $\left(\frac{a}{A}\right)=+1$, so behaupte ich, dafs daraus auch $\left(\frac{A}{a}\right)=+1$ folge. Ist nämlich β eine Primzahl von der Form $4n+3$, welche in der Formel x^2+a aufgeht, so mufs $\left(\frac{a}{\beta}\right)=-1$, und somit nach Fall I $\left(\frac{\beta}{a}\right)=-1$ sein. Betrachten wir die nicht erfüllbare Gleichung $x^2+ay^2=A\beta z^2$, so zeigt No. 27, dafs diese Gleichung stattfinden würde, wenn man zwei ganze Zahlen λ und μ von der Beschaffenheit finden könnte, dafs $\frac{\lambda^2+a}{A\beta}$ und $\frac{\mu^2-A\beta}{a}$ ganze Zahlen würden. Die erste Bedingung ist von selbst erfüllt; denn damit λ^2+a durch A teilbar sei, mufs $\left(\frac{-a}{A}\right)=1$ oder $\left(\frac{a}{A}\right)=1$ sein, und dies ist nach Voraussetzung der Fall; und damit λ^2+a durch β teilbar sei, mufs $\left(\frac{-a}{\beta}\right)=1$ oder $\left(\frac{a}{\beta}\right)=-1$ sein, was ebenfalls stattfindet.

Die zweite Bedingung würde erfordern, dafs $\left(\frac{A\beta}{a}\right)=+1$ oder

$\left(\frac{A}{a}\right)\left(\frac{\beta}{a}\right) = +1$ sei. Nun ist aber schon $\left(\frac{\beta}{a}\right) = -1$; mithin müſste $\left(\frac{A}{a}\right) = -1$ sein. Diese zweite Bedingung kann nicht erfüllt werden, da die gegebene Gleichung unmöglich ist. Demnach ist $\left(\frac{A}{a}\right) = +1$ und daher:

V. Ist $\left(\frac{a}{A}\right) = +1$, so ergiebt sich $\left(\frac{A}{a}\right) = +1$.

Ist jetzt $\left(\frac{a}{A}\right) = -1$, so kann nicht $\left(\frac{A}{a}\right) = +1$ sein, denn aus dieser würde sich für den soeben bewiesenen Fall $\left(\frac{a}{A}\right) = +1$ ergeben, was der Voraussetzung zuwider ist. Man hat daher $\left(\frac{A}{a}\right) = -1$ und somit:

VI. Ist $\left(\frac{a}{A}\right) = -1$, so ergiebt sich $\left(\frac{A}{a}\right) = -1$.

Wir haben oben in No. 48 bewiesen, daſs, wenn a und A zwei Primzahlen von der Form $4n+1$ sind, es immer möglich ist, einer der beiden Gleichungen $Ax^2 - ay^2 = \pm 1$, $x^2 - Aay^2 = -1$ zu genügen. Die erste erfordert, daſs man $\left(\frac{A}{a}\right) = +1$ und $\left(\frac{a}{A}\right) = +1$ habe. Wenn demnach $\left(\frac{A}{a}\right) = -1$ und $\left(\frac{a}{A}\right) = -1$ ist, Bedingungen, von denen die eine eine Folge der andern ist, wie wir soeben bewiesen haben, so ist die zweite Gleichung die einzig mögliche, und dieselbe findet notwendigerweise statt. Daraus folgt der Satz:

Sind a und A zwei Primzahlen von der Form $4n+1$, und ist $\left(\frac{A}{a}\right) = -1$ oder $\left(\frac{a}{A}\right) = -1$, so ist die Gleichung $x^2 - Aay^2 = -1$ immer möglich.

170.

Beweis der Fälle VII und VIII.

Ist $\left(\frac{a}{b}\right) = +1$, so behaupte ich, daſs daraus $\left(\frac{b}{a}\right) = +1$ folgt. Ist nämlich wieder β eine Primzahl von der Form $4n+3$, welche in der Formel $x^2 + a$ aufgeht, so daſs $\left(\frac{a}{\beta}\right) = -1$, und mithin $\left(\frac{\beta}{a}\right) = -1$ ist, so ist es, wie wir bereits in No. 49 gesehen haben, immer möglich, einer der drei folgenden Gleichungen

$$\pm 1 = ax^2 - b\beta y^2$$
$$\pm 1 = bx^2 - a\beta y^2$$
$$\pm 1 = \beta x^2 - aby^2,$$

vorausgesetzt, dafs man das Zeichen der linken Seite passend wählt, Genüge zu leisten.

Da nun $\left(\frac{a}{b}\right) = +1$, $\left(\frac{a}{\beta}\right) = -1$ und somit $\left(\frac{\beta}{a}\right) = -1$ angenommen worden ist, so ergiebt sich, dafs von diesen drei Gleichungen, welche eigentlich sechs darstellen, vier nicht stattfinden können, nämlich:

1) die Gleichung $+1 = \beta x^2 - aby^2$, welche $\left(\frac{\beta}{a}\right) = +1$ voraussetzt;

2) die Gleichung $-1 = \beta x^2 - aby^2$, welche $\left(\frac{\beta}{a}\right) = +1$ voraussetzt;

3) die Gleichung $-1 = ax^2 - b\beta y^2$, welche $\left(\frac{a}{b}\right) = -1$ voraussetzt;

4) die Gleichung $+1 = ax^2 - b\beta y^2$, welche $\left(\frac{a}{\beta}\right) = +1$ voraussetzt.

Es bleiben daher nur noch die beiden Gleichungen übrig:

$$+1 = bx^2 - a\beta y^2$$
$$-1 = bx^2 - a\beta y^2,$$

von denen eine notwendig stattfinden mufs. Nun erfordern alle beide, dafs $\left(\frac{b}{a}\right) = +1$ sei, da vermöge der ersten a ein Teiler von $b^2x^2 - b$ oder von $z^2 - b$ und vermöge der zweiten a ein Teiler von $b^2x^2 + b$ oder von $z^2 + b$ ist. Folglich:

VII. Ist $\left(\frac{a}{b}\right) = +1$, so ergiebt sich daraus $\left(\frac{b}{a}\right) = +1$.

Ist zweitens $\left(\frac{b}{a}\right) = -1$, so behaupte ich, dafs daraus $\left(\frac{a}{b}\right) = -1$ folgt. Denn hätte man $\left(\frac{a}{b}\right) = +1$, so würde daraus, entgegen unsrer Voraussetzung, nach dem eben bewiesenen Falle $\left(\frac{b}{a}\right) = +1$ folgen. Demnach erhält man schliesslich das Resultat:

VIII. Ist $\left(\frac{b}{a}\right) = -1$, so ergiebt sich daraus $\left(\frac{a}{b}\right) = -1$.

171.

Man bemerke, dafs die vier ersten Fälle auf eine vollkommene Weise, welche nichts zu wünschen übrig läfst, bewiesen sind. Die vier andern Fälle setzen voraus, dafs, wenn eine Zahl a von der

Form $4n+1$ gegeben ist, es immer möglich ist, eine Primzahl β von der Form $4n+3$ zu finden, welche in der Formel x^2+a aufgeht, und dafs somit $\left(\frac{a}{\beta}\right) = -1$ sei.

Die Existenz dieser Hülfsgröfse kann man unmittelbar beweisen, wenn a von der Form $8n+5$ ist. Denn setzt man $x=1$, so ist die Zahl x^2+a, welche in $1+a$ übergeht, von der Form $8n+6$; dieselbe ist daher teilbar durch eine Zahl von der Form $4n+3$, und daher auch durch eine Primzahl von eben dieser Form. Diese Primzahl kann dann für β genommen werden.

Ist a von der Form $8n+1$, so beachte man, dafs diese Form, in Bezug auf die Vielfachen von 3 betrachtet, sich in zwei andere spaltet, nämlich in $24n+1$ und $24n+17$. Hinsichtlich dieser letzteren braucht man nur $x=1$ zu setzen, und da x^2+a, welches in $24n+18$ übergeht, durch 3 teilbar ist, so kann man $\beta = 3$ nehmen. Alsdann ist die Bedingung $\left(\frac{a}{\beta}\right) = -1$ für jede Primzahl a von der Form $24n+17$ erfüllt.

Es ist daher nur noch zu beweisen, dafs man für jede Primzahl a von der Form $24n+1$, die Einheit ausgenommen, immer eine Primzahl β von der Form $4n+3$ finden kann, welche ein Teiler von z^2+a ist, oder welche der Bedingung $\left(\frac{a}{\beta}\right) = -1$ genügt.

Zunächst beweist man leicht durch eine einfache Substitution, dafs jede in einer der sechs Formen

$$a = 168x + 17,\ 41,\ 73,\ 89,\ 97,\ 145$$

enthaltene Primzahl von der Form $24n+1$ die Eigenschaft besitzt, dafs, wenn man entsprechend für z die Werte

$$z = 2,\ 1,\ 2,\ 3,\ 1,\ 3$$

nimmt, die Formel z^2+a durch 7 teilbar ist, so dafs der Wert $\beta = 7$ für alle in diesen Formeln enthaltenen Primzahlen der Bedingung $\left(\frac{a}{\beta}\right) = -1$ genügt.

Ebenso beweist man, dafs jede Primzahl von der Form $24n+1$, welche in einer der zehn Formen

$$a = 264x + 17,\ 41,\ 65,\ 73,\ 145,\ 161,\ 193,\ 217,\ 233,\ 241$$

enthalten ist, die Eigenschaft besitzt, dafs, wenn man entsprechend für z die Werte

$$z = 4,\ 5,\ 1,\ 2,\ 3,\ 2,\ 4,\ 5,\ 3,\ 1$$



setzt, die Formel $z^2 + a$ durch 11 teilbar ist. Setzt man also $\beta = 11$, so genügt man für alle Primzahlen a der Bedingung $\left(\frac{a}{\beta}\right) = -1$.

Primzahlen von der Form $24n + 1$ giebt es bis zur Grenze 1009 im Ganzen 15, nämlich:

$$73,\ 97,\ 193,\ 241,\ 313,\ 337,\ 409,\ 433,\ 457,\ 577,\ 601,\ 673,\ 769,\ 937,\ 1009.$$

Von diesen fünfzehn Zahlen genügen zehn der Bedingung $\left(\frac{a}{7}\right) = -1$, nämlich:

$$a = 73,\ 97,\ 241,\ 313,\ 409,\ 433,\ 577,\ 601,\ 769,\ 937,$$

die andern fünf der Bedingung $\left(\frac{a}{11}\right) = -1$, nämlich:

$$a = 193,\ 337,\ 457,\ 673,\ 1009.$$

Unsere Annahme ist daher bis zur Grenze $a = 1009$ als richtig bestätigt; dieselbe ist auch richtig für eine unendliche Anzahl von Primzahlen, welche in den vorhergehenden Formeln enthalten sind; indessen ist es von Wichtigkeit zu zeigen, daſs sie allgemein für jede Primzahl a von der Form $8n + 1$ auſser der Einheit richtig ist.

Wenn die Primzahl a von der Form $8n + 1$ ist, so weiſs man, daſs es immer möglich ist, der Gleichung $a = 2f^2 - g^2$ zu genügen, und daſs somit $2fy^2 + 2gyz + fz^2$ ein quadratischer Teiler der Formel $t^2 + au^2$ ist.

Wenn f eine Primzahl β von der Form $4n + 3$ zum Teiler hat (was immer der Fall ist, wenn f von dieser Form ist), so wird offenbar diese Zahl in $z^2 + a$, welches dadurch, daſs man $z = g$ setzt, in $2f^2$ übergeht, aufgehen, und es wird somit β der Bedingung genügen.

Überhaupt muſs es, was auch f sein möge, unter den Zahlen, welche durch $2fy^2 + 2gyz + fz^2$ dargestellt werden, und deren es unendlich viele giebt, eine oder mehrere geben, die sich durch eine Primzahl von der Form $4n + 3$ teilen lassen.

Wenn nämlich alle durch $2fy^2 + 2gyz + fz^2$ dargestellten Zahlen nur Primteiler von der Form $4n + 1$ besäſsen, so würde das Produkt aller, da jeder Teiler alsdann von der Form $p^2 + q^2$ wäre, selbst wenn man den Faktor 2 noch hinzunähme, von derselben Form sein. Mithin müſste man, welches auch die relativprimen Zahlen y und z sein mögen, stets der Gleichung

$$t^2 + u^2 = 2fy^2 + 2gyz + fz^2$$

genügen können. Die allgemeinste Art, dieser Gleichung Genüge zu



leisten, besteht darin, dafs man unbestimmte Zahlen A, B, M, N annimmt, und daraus die Werte bildet:

$$t = Ay + Bz, \quad u = My + Nz.$$

Alsdann müfste man die identische Gleichung haben:

$$(Ay + Bz)^2 + (My + Nz)^2 = 2fy^2 + 2gyz + fz^2,$$

und hieraus würden sich die drei Gleichungen ergeben:

$$\begin{aligned} A^2 + M^2 &= 2f \\ AB + MN &= g \\ B^2 + N^2 &= f, \end{aligned}$$

Multipliciert man die erste mit der dritten, und subtrahiert man von em Produkte das Quadrat der zweiten, so erhält man:

$$(AN - BM)^2 = 2f^2 - g^2 = a.$$

Es müfste demnach a ein Quadrat sein. Dies ist aber nicht der Fall, da a eine Primzahl und der Fall $a = 1$ ausgenommen ist.

Somit können nicht alle Primteiler der Formel $2fy^2 + 2gyz + fz^2$ von der Form $4n + 1$ sein; es giebt daher einen oder mehrere von der Form $4n + 3$. Ist β dieser Teiler oder einer von diesen Teilern, so kann man

$$\beta P = 2fy^2 + 2gyz + fz^2$$

oder:

$$\beta f P = (fz + gy)^2 + ay^2$$

setzen. Mithin ist β ein Teiler von $x^2 + a$.

Da übrigens der allgemeine Satz, welchen wir mit dem Namen **„Reciprocitätsgesetz zwischen zwei Primzahlen"** belegt haben, **der bemerkenswerteste und fruchtbarste Satz der Zahlentheorie** ist, so werden wir später noch einen zweiten Beweis desselben geben, der sich auf andere Prinzipien gründet.

172.

Es ist hier der Ort, um einige ziemlich wichtige Sätze anzuführen, von denen mehrere nur mit Hülfe des soeben bewiesenen Reciprocitätsgesetzes bewiesen werden können.

Jede Primzahl von der Form $4n + 1$ geht entweder gleichzeitig in den beiden Formeln $t^2 + cu^2$, $t^2 - cu^2$ oder in keiner von beiden auf.

Ist a die betreffende Primzahl, und hat man $\left(\frac{c}{a}\right) = +1$, so wird die Zahl a in den beiden Formeln $t^2 + cu^2$, $t^2 - cu^2$, in denen c

eine beliebige Zahl ist, aufgehen. Ist dagegen $\left(\frac{c}{a}\right) = -1$, so geht sie weder in der einen noch in der andern auf, wie sich unmittelbar aus No. 134 und 135 ergiebt.

173.

Jede Primzahl von der Form $4n + 3$, welche in $t^2 + cu^2$ aufgeht, kann nicht in $t^2 - cu^2$ aufgehen und umgekehrt.

Denn ist diese Primzahl gleich b, so ist die Bedingung dafür, dafs b in $t^2 + cu^2$ aufgehe: $\left(\frac{-c}{b}\right) = 1$ oder $\left(\frac{c}{b}\right) = -1$, und die Bedingung, dafs sie in $t^2 - cu^2$ aufgehe, ist $\left(\frac{c}{b}\right) = +1$. Diese beiden Bedingungen schliefsen sich aber gegenseitig aus.

Zusatz. Jede Primzahl b von der Form $4n + 3$ ist notwendig ein Teiler einer der beiden Formeln $t^2 + cu^2$, $t^2 - cu^2$; denn es ist immer entweder $\left(\frac{c}{b}\right) = +1$ oder $\left(\frac{c}{b}\right) = -1$. Bei diesem und dem vorhergehenden Satze sieht man von dem Falle ab, wo b ein Teiler von c ist. Alsdann brauchte man nämlich nicht mehr zu fragen, ob b in $t^2 + cu^2$ oder in $t^2 - cu^2$ aufgehe.

174.

Wenn die Primzahl c in den beiden Formeln $t^2 - au^2$ und $t^2 - bu^2$ aufgeht, so geht sie auch in der Formel $t^2 - abu^2$ auf.

Denn da nach Voraussetzung $\left(\frac{a}{c}\right) = 1$ und $\left(\frac{b}{c}\right) = 1$ ist, so folgt daraus $\left(\frac{ab}{c}\right) = 1$, und somit ist c ein Teiler von $t^2 - abu^2$.

Dasselbe Resultat würde für eine gröfsere Anzahl von Faktoren stattfinden.

175.

Wenn die Primzahl c weder in der Formel $t^2 - au^2$ noch in der Formel $t^2 - bu^2$ aufgeht, so geht sie notwendig in der Formel $t^2 - abu^2$ auf.

Denn da nach Voraussetzung $\left(\frac{a}{c}\right) = -1$ und $\left(\frac{b}{c}\right) = -1$ ist, so folgt daraus $\left(\frac{ab}{c}\right) = +1$, und somit ist c ein Teiler von $t^2 - abu^2$.

176.

Sind a und A zwei Primzahlen, beide von der Form $4n + 1$, so wird, wenn a in der Formel $t^2 + Au^2$ aufgeht, umgekehrt A

in der Formel $t^2 + au^2$ aufgehen. Geht aber a nicht in der Formel $t^2 + Au^2$ auf, so wird auch umgekehrt A nicht in der Formel $t^2 + au^2$ aufgehen.

Im ersten Falle ist nämlich $\left(\frac{-A}{a}\right) = 1$, d. h. $\left(\frac{A}{a}\right) = 1$, also umgekehrt $\left(\frac{a}{A}\right) = 1$. Folglich ist A ein Teiler von $t^2 + au^2$.

Im zweiten Falle ist $\left(\frac{A}{a}\right) = -1$; daraus folgt ebenfalls $\left(\frac{a}{A}\right) = -1$; mithin ist A kein Teiler von $t^2 + au^2$.

177.

Ist a eine Primzahl von der Form $4n + 1$, und sind A und B zwei beliebige Primzahlen, welche entweder alle beide Teiler oder alle beide Nicht-Teiler der Formel $t^2 - au^2$ sind, so ist a ein Teiler der Formel $t^2 - ABu^2$.

1) Sind nämlich A und B Teiler der Formel $t^2 - au^2$, so hat man $\left(\frac{a}{A}\right) = 1$, $\left(\frac{a}{B}\right) = 1$ und daher umgekehrt $\left(\frac{A}{a}\right) = 1$, $\left(\frac{B}{a}\right) = 1$. Mithin $\left(\frac{AB}{a}\right) = 1$. Folglich ist a ein Teiler von $t^2 - ABu^2$.

2) Sind A und B keine Teiler der Formel $t^2 - au^2$, so ist $\left(\frac{a}{A}\right) = -1$, $\left(\frac{a}{B}\right) = -1$ und daher umgekehrt $\left(\frac{A}{a}\right) = -1$, $\left(\frac{B}{a}\right) = -1$. Mithin ebenfalls $\left(\frac{AB}{a}\right) = 1$. Folglich ist a ein Teiler von $t^2 - ABu^2$.

178.

Ist a eine Primzahl von der Form $4n + 1$ und b eine solche von der Form $4n + 3$, welche nicht ein Teiler von $t^2 + au^2$ ist, so wird im Gegenteil a ein Teiler von $t^2 + bu^2$ sein.

Denn da nach Voraussetzung $\left(\frac{-a}{b}\right) = -1$ oder $\left(\frac{a}{b}\right) = +1$ ist, so folgt daraus $\left(\frac{b}{a}\right) = 1$. Folglich ist a ein Teiler von $t^2 + bu^2$.

Hat man allgemein mehrere Primzahlen b, b', b'', alle von der Form $4n + 3$, von denen keine in $x^2 + a$ aufgeht, so ist a ein Teiler der Formel $t^2 + bb'b''u^2$.

179.

Jede Primzahl c von der Form $8n + 1$ oder $8n + 7$ geht entweder gleichzeitig in den beiden Formeln $t^2 + au^2$ und $t^2 + 2au^2$ oder in keiner von beiden auf.

Denn der Wert von $\left(\frac{-a}{c}\right)$ ist derselbe, wie der von $\left(\frac{-2a}{c}\right)$, da man stets, wenn die Zahl c von einer der erwähnten Formen ist, nach No. 150 $\left(\frac{2}{c}\right) = 1$ hat.

180.

Jede Primzahl c von der Form $8n + 3$ oder $8n + 5$ geht stets in einer, aber auch nur in einer der beiden Formeln $t^2 + au^2$, $t^2 + 2au^2$ auf.

Denn bei den erwähnten Formen hat man $\left(\frac{2}{c}\right) = -1$; mithin sind die beiden Gröſsen $\left(\frac{-a}{c}\right)$ und $\left(\frac{-2a}{c}\right)$ von entgegengesetztem Zeichen. Es muſs demnach die eine dieser Gröſsen $+1$, die andere -1 sein. Daraus folgt, daſs c in der einen von den beiden in Rede stehenden Formeln aufgeht, nicht aber in der andern.

Man beachte, daſs in diesem Satze, ebenso wie im vorhergehenden, a irgend eine positive oder negative Zahl ist.

181.

Wir halten uns nicht länger damit auf, diese Art von Sätzen noch weiter zu vermehren; doch, glauben wir, werden die Mathematiker mit Vergnügen die Anwendung unseres Reciprocitätsgesetzes auf den Beweis zweier allgemeinen Sätze sehen, zu denen Euler auf dem Wege der Induktion in seinen Opuscula analytica Bd. I gelangt ist, und die die Grundlage einer wichtigen Theorie bilden. Der erste ist ungefähr in folgende Worte gefaſst (s. das angeführte Werk S. 276):

Wenn man die aufeinanderfolgenden Quadratzahlen 1, 4, 9 16, . . . sämtlich durch eine und dieselbe Primzahl von der Form $4n + 1$ dividiert, so werden die bei der Division sich ergebenden Reste nicht nur alle Zahlen, welche in den Formeln $n - q^2 - q$ und $q^2 + q - n$ enthalten sind, sondern auch alle Primfaktoren, aus denen diese Zahlen zusammengesetzt sind, umfassen.

Zunächst sieht man leicht, daſs man, da $c = 4n + 1$ ist, der Gleichung

$$\frac{x^2 + n - q^2 - q}{c} = e$$

dadurch genügen kann, daſs man $2x = 2q + 1 \pm c$ setzt. Da ferner c von der Form $4n + 1$ ist, so ist, falls die Gleichung $\frac{x^2 + a}{c} = e$

möglich ist, die Gleichung $\frac{y^2 - a}{c} = e$ ebenfalls möglich. Mithin kann in der That jede Zahl, welche entweder in der Formel $n - q^2 - q$ oder in der Formel $q^2 + q - n$ enthalten ist, oder die um ein Vielfaches von c verminderte Zahl dieser Art als der Rest angesehen werden, welcher bei der Division einer Quadratzahl durch c übrigbleibt. Dieser erste Teil des Satzes bietet, wie Euler selbst gezeigt hat, keine Schwierigkeiten. Wir gehen zu dem zweiten Teile, welcher die Anwendung des Reciprocitätsgesetzes erfordert, über.

Ist α eine Primzahl, welche in $n - q^2 - q$ oder in $q^2 + q - n$ aufgeht, so kann man $q^2 + q - n = \pm \alpha A$ setzen. Multipliciert man also mit 4 und setzt dann für $4n$ seinen Wert $c - 1$, so hat man:

$$(2q + 1)^2 - c = \pm 4\alpha A.$$

Hieraus ergiebt sich, wenn die Vielfachen von α weggelassen werden, $c = (2q + 1)^2$. Mithin ist $c^{\frac{\alpha - 1}{2}}$ oder nach unsrer Bezeichnung $\left(\frac{c}{\alpha}\right) = (2q + 1)^{\alpha - 1} = 1$. Aus $\left(\frac{c}{\alpha}\right) = 1$ folgt aber nach dem Reciprocitätsgesetze $\left(\frac{\alpha}{c}\right) = 1$. Demnach ist c ein Teiler der Formel $x^2 - \alpha$. Somit mufs sich α unter den Resten, welche bei der Division der Quadratzahlen durch die Primzahl c übrig bleiben, vorfinden. Dies ist der Satz von Euler.

182.

Der zweite allgemeine Satz (s. das angeführte Werk S. 281) ist der folgende:

Wenn man die Quadratzahlen 1, 4, 9, 16, . . . durch die Primzahl $4n - 1$ dividiert, so werden die bei der Division sich ergebenden Reste nicht nur alle durch die Formel $n + q^2 + q$ dargestellten Zahlen, sondern auch alle Primfaktoren, aus denen diese Zahlen zusammengesetzt sind, enthalten.

Um dem ersten Teile zu genügen, mufs man eine Zahl x von der Beschaffenheit finden, dafs $x^2 - (n + q^2 + q)$ durch die Primzahl $c = 4n - 1$ teilbar ist. Dies erreicht man aber unmittelbar, wenn man $2x = 2q + 1 \pm c$ setzt. Mithin ist die Zahl $n + q^2 + q$ oder diese um ein Vielfaches von c verminderte Zahl stets der Rest, welchen die Quadratzahl x^2 bei der Division durch c übrigläfst.

Ist ferner α eine Primzahl, welche in $n + q^2 + q$ aufgeht und setzt man $n + q^2 + q = \alpha A$, so leitet man daraus, ebenso wie oben,



die Gleichung $(2q+1)^2 + c = 4\alpha A$ ab. Läſst man also die Vielfachen von α weg, so hat man $c = -(2q+1)^2$, also $\left(\frac{-c}{\alpha}\right) = 1$. Hiernach sind zwei Fälle zu unterscheiden.

1) Ist α von der Form $4m+1$, so ist die Gleichung $\left(\frac{-c}{\alpha}\right) = 1$ dieselbe wie $\left(\frac{c}{\alpha}\right) = 1$; daraus folgt nach dem Reciprocitätsgesetze $\left(\frac{\alpha}{c}\right) = 1$. Mithin ist c ein Teiler von $x^2 - \alpha$.

2) Ist α von der Form $4m-1$, so giebt die Gleichung $\left(\frac{-c}{\alpha}\right) = 1$ die folgende $\left(\frac{c}{\alpha}\right) = -1$. Daraus folgt nach dem Reciprocitätsgesetze $\left(\frac{\alpha}{c}\right) = 1$. Mithin ist auch hier c ein Teiler von $x^2 - \alpha$.

Demnach ist in allen Fällen die Primzahl α, oder diese Zahl vermindert um ein Vielfaches von c der Rest, welchen eine Quadratzahl bei der Division durch c übrigläſst; es muſs sich daher jene Zahl unter den Resten, welche die verschiedenen Glieder der Reihe 1, 4, 9, 16, . . . bei der Division durch c ergeben, vorfinden.

§ 7.

Anwendung des vorigen Satzes, um zu erkennen, ob eine Primzahl c in der Formel $x^2 + a$ aufgeht. Fälle, in denen man die Zahl x a priori bestimmen kann.

183.

Wenn c eine etwas groſse Zahl ist und man wissen will, ob c ein Teiler von $x^2 + a$ sei, so kann die Erhebung der Zahl a auf die Potenz $\frac{c-1}{2}$ sehr langwierig sein, selbst wenn man die Rechnung soviel wie möglich abkürzt und darauf achtet, daſs die Vielfachen von c, so oft sie sich darbieten, weggelassen werden. Ein Verfahren, welches der vorhergehende Satz an die Hand giebt, und welches sehr schnell zu dem gesuchten Werte von $\left(\frac{a}{c}\right)$ führt, ist folgendes:

1) Ist a gröſser als c, so setze man an Stelle von a den Rest der Division von a durch c. Mithin kann man immer annehmen, daſs a kleiner als c sei. In der That sieht man sofort, daſs $(mc+\alpha)^{\frac{c-1}{2}}$ bei der Division durch c denselben Rest läſst wie $\alpha^{\frac{c-1}{2}}$.

2) Wenn die so reducierte Zahl a eine Primzahl ist, so

verwandelt sich der Ausdruck $\left(\frac{a}{c}\right)$ unserm Satze zufolge entweder in $\left(\frac{c}{a}\right)$ oder in $-\left(\frac{c}{a}\right)$, und zwar kann dieser letztere Fall nur eintreten, wenn a und c alle beide von der Form $4n+3$ sind. Da aber $c>a$ ist, so kann man an Stelle von c den Rest der Division von c durch a setzen. Ist dieser Rest c', so hat man also $\left(\frac{c}{a}\right)=\left(\frac{c'}{a}\right)$. Somit ist die Untersuchung des Wertes von $\left(\frac{a}{c}\right)$ zurückgeführt auf diejenige des Ausdruckes $\left(\frac{c'}{a}\right)$, welcher aus kleineren Zahlen besteht. Die fernere Ermittlung des Wertes geschieht daher teils nach dem, was wir bereits erwähnt haben, teils nach dem, was wir noch hinzufügen werden.

3) Ist a keine Primzahl, so zerlege man dieselbe in ihre Primfaktoren $\alpha, \beta, \gamma, \ldots$, unter denen auch 2 enthalten sein kann. Dann ist $\left(\frac{a}{c}\right)$ gleich dem Produkte $\left(\frac{\alpha}{c}\right)\left(\frac{\beta}{c}\right)\left(\frac{\gamma}{c}\right)\cdots$ Von den Faktoren $\alpha, \beta, \gamma, \ldots$ lasse man diejenigen weg, welche Quadrate sind, da allgemein $\left(\frac{\alpha^2}{c}\right)=\left(\frac{\alpha}{c}\right)\left(\frac{\alpha}{c}\right)=+1$ ist. Ferner beachte man, dafs nach No. 150 $\left(\frac{2}{c}\right)=+1$, sobald c die Form $8n\pm 1$, und $\left(\frac{2}{c}\right)=-1$ ist, sobald c die Form $8n\pm 3$ besitzt.

Mit Hülfe dieser Vorschriften und Umkehrungen, wie sie durch den Satz des vorhergehenden Paragraphen gegeben sind, findet man bald den Wert des gegebenen Ausdrucks $\left(\frac{a}{c}\right)$. Die Rechnung, die derjenigen ziemlich ähnlich ist, mittelst welcher man den gröfsten gemeinschaftlichen Teiler zweier Zahlen sucht, ist nahezu ebenso leicht und einfach wie diese.

184.

Beispiel 1.

Um den Wert des Ausdrucks $\left(\frac{601}{1013}\right)$ zu erhalten, bemerken wir, dafs diese beiden Zahlen Primzahlen sind. Unserm Satze zufolge erhalten wir also:

$$\left(\frac{601}{1013}\right)=\left(\frac{1013}{601}\right).$$

Die Division von 1013 durch 601 giebt 412 als Rest, und da 412

das Produkt aus 4 und 103 ist, so kann man den quadratischen Faktor 4 weglassen. Dies giebt:

$$\left(\frac{601}{1013}\right) = \left(\frac{103}{601}\right).$$

Da aber 103 ebenfalls eine Primzahl ist, so hat man nach unserm Satze:

$$\left(\frac{103}{601}\right) = \left(\frac{601}{103}\right),$$

und wenn man 601 durch 103 dividiert und nur den Rest beibehält:

$$= \left(\frac{86}{103}\right) = \left(\frac{-17}{103}\right) = -\left(\frac{17}{103}\right) = -\left(\frac{103}{17}\right) = -\left(\frac{1}{17}\right) = -1.$$

Mithin ist:

$$\left(\frac{601}{1013}\right) = -1.$$

Demnach ist 1013 kein Teiler von $x^2 + 601$.

Um dieselbe Ermittlung des Wertes auf dem gewöhnlichen Wege auszuführen, hätte man 601 auf die Potenz 506 erheben müssen, indem man die Vielfachen von 1013, so oft sie vorkommen, wegläſst. Die Zahl 506 ist aber im dyadischen Zahlsystem*) ausgedrückt 111 111 010 d. h. in andern Worten 506 ist die Summe der Potenzen von 2, deren Exponenten 8, 7, 6, 5, 4, 3, 1 sind. Um die Potenzen von 601, welche diese Potenzen von 2 zu Exponenten haben, zu bilden, muſs man acht Multiplikationen oder Erhebungen zum Quadrat ausführen; darauf bedarf es, um die verschiedenen Potenzen von 601, deren Exponenten 2^8, 2^7, 2^6, 2^5, 2^4, 2^3, 2^1 sind, mit einander zu multiplicieren, noch weiterer sechs Multiplikationen, so daſs man, um zum schlieſslichen Resultat zu kommen, vierzehn Multiplikationen und ebenso viele Divisionen durch 1013 nötig hat. Im Übrigen sind behufs besserer Vergleichung der beiden Methoden die Einzelheiten der Rechnung folgende, wobei nur die Reste der Divisionen durch 1013 hingeschrieben sind:

---

*) Ein sehr kurzes Verfahren, eine etwas groſse Zahl im dyadischen Zahlsystem auszudrücken, ist folgendes: Ist z. B. die Zahl 11183445 gegeben, von der im Beispiel 3 die Rede sein wird, so dividiere man diese Zahl durch 64; dies giebt den Rest 21 und den Quotienten 174741; dieser, durch 64 geteilt, giebt den Rest 21 und den Quotienten 2730; endlich giebt 2730 durch 64 geteilt den Rest 42 und den Quotienten 42. Nun drückt sich aber 21 im dyadischen Zahlsystem durch 10101 und 42 durch 101010 aus; mithin wird die gegebene Zahl durch 101010 101010 010101 010101 ausgedrückt.

Anmerkung des Verfassers.

$$
\begin{aligned}
(601)^2 &= 573 \\
(601)^4 &= (573)^2 = 117 \\
(601)^8 &= (117)^2 = 520 \\
(601)^{16} &= (520)^2 = -71 \\
(601)^{32} &= (71)^2 = -24 \\
(601)^{64} &= (24)^2 = -437 \\
(601)^{128} &= (437)^2 = 525 \\
(601)^{256} &= (525)^2 = 89
\end{aligned}
$$

$$
\begin{aligned}
(601)^{384} &= 89 \times 525 = 127 \\
(601)^{448} &= 127 \times -437 = +216 \\
(601)^{480} &= +216 \times -24 = -119 \\
(601)^{496} &= -119 \times -71 = 345 \\
(601)^{504} &= 345 \times 520 = 99 \\
(601)^{506} &= 99 \times 573 = -1.
\end{aligned}
$$

Demnach ist in der That:

$$\left(\frac{601}{1013}\right) = -1.$$

185.

Beispiel 2.

Man soll den Wert von $\left(\frac{402}{929}\right)$ finden.

Dazu zerlege man 402 in seine drei Faktoren 2 . 3 . 67. Dann erhält man:

$$\left(\frac{402}{929}\right) = \left(\frac{2}{929}\right) \cdot \left(\frac{3}{929}\right) \cdot \left(\frac{67}{929}\right).$$

Nun ist aber:

$$
\begin{aligned}
&\left(\frac{2}{929}\right) = 1 \\
&\left(\frac{3}{929}\right) = \left(\frac{929}{3}\right) = \left(\frac{2}{3}\right) = -1 \\
&\left(\frac{67}{929}\right) = \left(\frac{929}{67}\right) = \left(\frac{-9}{67}\right) = -\left(\frac{1}{67}\right) = -1.
\end{aligned}
$$

Das Produkt dieser drei Resultate ist $+1$; mithin ist:

$$\left(\frac{402}{929}\right) = +1.$$

Es ist demnach 929 ein Teiler von $t^2 \pm 402u^2$ oder von $x^2 \pm 402$.

186.

Beispiel 3.

Wir nehmen noch eine sehr grofse Primzahl z. B. 22 366 891 und untersuchen, ob diese Zahl ein Teiler von $x^2 + 1459$ ist.

Dazu mufs man den Wert von $\left(\frac{1459}{22\,366\,891}\right)$ wissen. Da nun 1459 gleichfalls eine Primzahl von der Form $4n + 3$ ist, so ist dieser Wert:

$$= -\left(\frac{22\,366\,891}{1459}\right) = -\left(\frac{421}{1459}\right) = -\left(\frac{1459}{421}\right) = -\left(\frac{196}{421}\right) = -1,$$

(weil 196 eine Quadratzahl ist). Demnach ist der gesuchte Wert gleich -1. Es ist daher 22 366 891 ein Teiler von $x^2 + 1459$.

Dies hätte man auf dem gewöhnlichen Wege nur durch Ausführung von 34 Multiplikationen und ebenso vieler, wegen des Divisors 22 366 891 sehr mühsamer Divisionen finden können.

187.

Nachdem man nun die Gewifsheit erlangt hat, dafs die Primzahl c ein Teiler von $x^2 + a$ ist, hat man noch den Wert von x zu bestimmen, welcher die Division ausführbar macht. Dies kann in einigen allgemeinen Fällen, die wir anführen wollen, a priori geschehen.

1) Ist $c = 4n + 3$, so ist die Bedingung der Möglichkeit der Division, dafs $(-a)^{2n+1} - 1$ durch c teilbar sei. Mithin ist $a^{2n+2} + a$ durch c teilbar. Nimmt man also $x = a^{n+1}$ oder gleich dem Reste, welchen a^{n+1} bei der Division durch c läfst, so ist man sicher, dafs $\frac{x^2 + a}{c}$ eine ganze Zahl ist. Dieser erste sehr allgemeine Fall umfafst bereits die Hälfte aller möglichen Fälle. Es bleibt daher nur noch der Fall $c = 4n + 1$, welcher die beiden Formen $8n + 1$ und $8n + 5$ einschliefst, zu untersuchen übrig.

2) Ist $c = 8n + 5$, so erfordert die Bedingung der Möglichkeit, dafs $a^{4n+2} - 1$ durch c teilbar sei. Diese Gröfse ist aber das Produkt der beiden Faktoren $a^{2n+1} + 1$ und $a^{2n+1} - 1$; somit mufs einer dieser Faktoren durch c teilbar sein. Ist der Faktor $a^{2n+1} + 1$ durch c teilbar, so setze man $x = a^{n+1}$, wodurch $\frac{x^2 + a}{c} = e$ wird. Ist aber der andere Faktor durch c teilbar, so setze man ebenso $\vartheta = a^{n+1}$; dann ist $\frac{\vartheta^2 - a}{c} = e$. In diesem letzteren Falle hat man also nur

noch der Gleichung $\frac{x^2 + \vartheta^2}{c} = e$ zu genügen. Nun kann man, da c von der Form $4m + 1$ ist, immer $c = f^2 + g^2$ setzen. Sucht man sodann die Unbestimmten p und q, welche der Gleichung

$$\vartheta = fp + gq$$

genügen, so folgt daraus:

$$x = fq - gp.$$

Denn hieraus ergiebt sich:

$$x^2 + \vartheta^2 = (f^2 + g^2)(p^2 + q^2).$$

Demnach ist $x^2 + \vartheta^2$, und folglich $x^2 + a$ teilbar durch c.

3) Der letzte zu betrachtende Fall ist $c = 8n + 1$. Alsdann aber kann man der Gleichung $\frac{x^2 + a}{c} = e$ nicht immer auf eine direkte Weise und ohne Probieren Genüge leisten. Ist $n = \alpha\beta$, wo β eine ungerade Zahl und α eine Potenz von 2 ist, so kann es, da die Bedingung der Möglichkeit erfordert, dafs $a^{4\alpha\beta} - 1$ durch c teilbar sei, vorkommen, dafs sich $a^\beta \pm 1$ durch c teilen läfst, und alsdann findet man, da β ungerade ist, den Wert von x gerade so, wie man ihn im Falle $c = 8n + 5$ gefunden hatte.

Ist $a^\beta \pm 1$ nicht durch c teilbar, so findet man keine Lösung a priori. Man mufs demnach, wenn man die Gleichung $\frac{x^2 + a}{c} = e$ auflösen will, die verschiedenen Glieder der Reihe $c - a$, $2c - a$, $3c - a$, $4c - a$, ... berechnen, bis man eines findet, das ein vollkommenes Quadrat ist und den Wert von x^2 giebt. Übrigens enthält diese Reihe notwendig das gesuchte Quadrat, und zwar mufs dieses kleiner als $\frac{1}{4}c^2$ sein, so dafs die Anzahl der zu berechnenden Glieder $\frac{1}{4}c$ nicht übersteigen kann.

Ist z. B. die Gleichung

$$\frac{x^2 + 229}{641} = e$$

gegeben, deren Möglichkeit durch die Bedingung $\left(\frac{229}{641}\right) = 1$ bereits festgestellt ist, so mufs man die verschiedenen Glieder der arithmetischen Progression, deren allgemeines Glied $641e - 229$ ist, bilden. Diese Progression ist:

$$412,\ 1053,\ 1694,\ 2335,\ \ldots$$

Indessen mufs man dieselbe bis zum 94ten Gliede fortsetzen, ehe man das Quadrat 60025, dessen Wurzel $x = 245$ ist, findet. Allerdings kann man viele Glieder unbeachtet lassen, wenn man vorhersieht,

dafs die Endziffer derselben keine von denen ist, die den Quadratzahlen eigen*) sind. Jedoch bleibt die Arbeit auf diesem Wege immer noch ziemlich langwierig, wenn die gesuchte Zahl x nicht viel kleiner als $\frac{1}{2}c$ ist.

188.

Um diese Bestimmung weniger mühsam zu machen, kann man sich auf Eigenschaften der Teiler stützen, die wir später beweisen werden. Diesen Eigenschaften zufolge ist jeder Teiler der Formel $t^2 + au^2$ selbst von der Form $y^2 + az^2$, oder er nimmt wenigstens diese Form an, wenn man ihn mit einer Zahl p, die kleiner als $2\sqrt{\frac{a}{3}}$ ist, multipliciert. Nimmt man an, dafs man $pc = f^2 + ag^2$ gefunden habe, so bestimme man x aus der Gleichung:

$$f = gx + cy.$$

Dann wird der Wert von x derart sein, dafs $x^2 + a$ durch c teilbar ist.

So erkennt man in dem vorigen Beispiel bald, dafs die Zahl 641 nicht von der Form $f^2 + 229g^2$ ist; sie wird es aber, nachdem man sie mit 14 multipliciert hat; denn es ist:

$$641 \times 14 = 8974 = 57^2 + 229 \,.\, 5^2.$$

Setzt man also $57 = 5x + 641y$, so findet man $x = -245$. Dieses Verfahren kann viele Versuche ersparen, und es wird besonders vorteilhaft, wenn a etwas beträchtlich ist. Die Tafeln zeigen nämlich je nach der Form $4az + a$ der Zahl c den Multiplikator an, vermittelst dessen das Produkt pc auf die Form $f^2 + ag^2$ gebracht wird.

---

*) Das Quadrat der Zahl $10m + n$ ist $100m^2 + 20mn + n^2$; mithin ist die Endziffer des Quadrats von $10m + n$ dieselbe wie die Endziffer des Quadrats von n. Nun haben aber die Quadrate der Zahlen 0, 1, 2, 3, . . . 9 zu Endziffern eine der Ziffern 0, 1, 4, 5, 6, 9; mithin kann kein Quadrat mit 2, 3, 7, 8 endigen.

Zu dieser Bemerkung kann man noch hinzufügen:

1) Wenn die letzte Ziffer eines Quadrates 0 ist, so müssen die letzten beiden Ziffern zwei Nullen sein.

2) Wenn die letzte Ziffer 5 ist, so müssen die beiden letzten 25 sein.

3) Wenn die letzte Ziffer ungerade ist, so mufs die vorletzte gerade sein.

4) Wenn die letzte Ziffer 4 ist, so mufs die vorletzte gerade sein, damit die ganze Zahl durch 4 teilbar sei.

5) Wenn die letzte Ziffer 6 ist, so mufs die vorletzte ungerade sein aus demselben Grunde. Anm. d. Verf.

§ 8.

Methode, um x so zu bestimmen, dafs $x^2 + a$ durch eine beliebige zusammengesetzte Zahl N teilbar sei.

189.

Ist c eine Primzahl und a irgend eine durch c nicht teilbare Zahl, und will man den Wert von x wissen, für welchen $x^2 + a$ durch c^m teilbar ist, so suche man zunächst nach dem Vorhergehenden den Wert von ϑ, für welchen $\vartheta^2 + a$ durch c teilbar ist, und setze sodann:

$$(\vartheta + \sqrt{-a})^m = p + q\sqrt{-a}.$$

Dann ist ebenso:

$$(\vartheta - \sqrt{-a})^m = p - q\sqrt{-a},$$

und das Produkt beider Gleichungen giebt:

$$(\vartheta^2 + a)^m = p^2 + aq^2.$$

Demnach ist $p^2 + aq^2$ durch c^m teilbar. In diesem Resultat sind q und c prim zu einander. Man kann daher

$$p = qx + c^m y$$

setzen, und es wird $x^2 + a$ durch c^m teilbar sein, was verlangt wurde.

Wir haben soeben vorausgesetzt, dafs q nicht durch c teilbar ist. Denn wäre dies der Fall, so würde p zufolge der Gleichung

$$(\vartheta^2 + a)^m = p^2 + aq^2,$$

deren linke Seite durch c^m teilbar ist, ebenfalls durch c teilbar sein. Es ist aber:

$$p = \vartheta^m - \frac{m(m-1)}{1 \cdot 2}\vartheta^{m-2}a + \frac{m(m-1)(m-2)(m-3)}{1 \cdot 2 \cdot 3 \cdot 4}\vartheta^{m-4}a^2 - \cdots,$$

und da $\vartheta^2 + a$ durch c teilbar ist, so kann man $-\vartheta^2 + Ac$ für a setzen, wodurch p von der Form wird:

$$p = \vartheta^m\left(1 + \frac{m(m-1)}{1 \cdot 2} + \frac{m(m-1)(m-2)(m-3)}{1 \cdot 2 \cdot 3 \cdot 4} + \cdots\right) + Bc,$$

oder:

$$p = 2^{m-1}\vartheta^m + Bc.$$

Nun ist aber ϑ nicht durch c teilbar, demnach kann auch nicht p und somit auch nicht q durch c teilbar sein.

Ist die Zahl a durch c teilbar, so ist die Gröfse $x^2 + a$ ebenfalls durch c teilbar, wenn man $x = 0$ oder gleich einem Vielfachen von c setzt. Es ist jedoch häufig unmöglich, dafs $x^2 + a$ durch c^2



oder durch eine höhere Potenz von c teilbar sei. Ist z. B. a durch c, aber nicht durch c^2 teilbar, so ist offenbar $x^2 + a$ niemals durch c^2 teilbar.

190.

Es ist nun leicht, den Wert von x, falls dies überhaupt möglich ist, zu finden, für welchen $x^2 + a$ durch irgend eine **zusammengesetzte** Zahl N teilbar ist.

1) Sind N und a relative Primzahlen, so zerlege man N in seine ungeraden Primfaktoren $\alpha^\lambda \beta^\mu \gamma^\nu \ldots$ und suche nach der vorstehenden Methode die Zahlen A, B, C, ..., für welche die Gröfsen

$$\frac{A^2 + a}{\alpha^\lambda}, \quad \frac{B^2 + a}{\beta^\mu}, \quad \frac{C^2 + a}{\gamma^\nu}, \ldots$$

ganze Zahlen werden. Sodann hat man den unbestimmten Gleichungen

$$x = A + \alpha^\lambda y = \pm B + \beta^\mu z = \pm C + \gamma^\nu u = \cdots$$

zu genügen, und man sieht leicht, dafs, wenn $x^2 + a$ durch jeden der Faktoren α^λ, β^μ, γ^ν, ... teilbar ist, es auch durch ihr Produkt $\alpha^\lambda \beta^\mu \gamma^\nu \ldots$ teilbar ist.

2) Sind die Zahlen N und a nicht prim zu einander, so sei $\psi^2 \omega$ ihr gröfster gemeinschaftlicher Teiler, wobei ψ^2 das gröfste in $\psi^2 \omega$ aufgehende Quadrat ist, und somit ω nur noch einfache Faktoren besitzen kann. Alsdann hat man zu setzen:

$$N = \psi^2 \omega N', \quad a = \psi^2 \omega a', \quad x = \psi \omega x'.$$

Dadurch geht die aufzulösende Gleichung $\frac{x^2 + a}{N} = e$ über in:

$$\frac{\omega x'^2 + a'}{N'} = e.$$

In dieser müssen ω und N' zu einander prim sein; denn wenn sie einen gemeinschaftlichen Teiler π hätten, so müfste auch a' durch π teilbar sein (da sonst die aufzulösende Gleichung unmöglich wäre). Mithin würde, entgegen unserer Annahme, $\omega \psi^2$ nicht der gröfste gemeinsame Teiler von a und N sein.

Da ω und N' prim zu einander sind, so kann man zwei ganze Zahlen f und g von der Beschaffenheit finden, dafs $f\omega - gN' = 1$ ist. Multipliciert man also die Gleichung $\frac{\omega x'^2 + a'}{N'} = e$ mit f und setzt $gN' + 1$ an die Stelle von $f\omega$, so geht diese Gleichung über in:

$$\frac{x'^2 + fa'}{N'} = e.$$

Mithin ist die Aufgabe auf den vorigen Fall zurückgeführt, in welchem N und a zu einander prim sind.

191.

Wenn die Zahl N aufser den in den vorhergehenden beiden Fällen betrachteten ungeraden Faktoren α^λ, β^μ, γ^ν, ... noch den Faktor 2^m enthält, so mufs man die für jeden ungeraden Faktor gefundenen Werte mit demjenigen verbinden, welcher aus der Gleichung

$$\frac{x^2 + a}{2^m} = e,$$

mit der wir uns sogleich beschäftigen werden, hervorgeht.

Ist a durch 4 oder durch eine höhere Potenz von 2 z. B. durch 2^{2i} oder 2^{2i+1} teilbar, so mufs man $x = 2^i x'$ setzen. Dadurch wird die Aufgabe unmittelbar auf den Fall zurückgeführt, wo a ungerade oder das Doppelte einer ungeraden Zahl ist.

Ist a das Doppelte einer ungeraden Zahl, so ist ersichtlich, dafs die Gleichung $x^2 + a = 2^m y$ nur in dem einen Falle $m = 1$ auflösbar ist, so dafs wir von diesem Falle absehen können.

Ist demnach a ungerade und $m > 1$, so mufs x ungerade sein, und da alsdann x^2 von der Form $8n + 1$ ist, so erhält man je nach den verschiedenen Formen von $a = \pm c$ die entsprechenden Formen von $x^2 \pm c$ wie folgt:

$$\begin{array}{lll} c = 8n + 1, & x^2 + c = 8n + 2, & x^2 - c = 8n \\ c = 8n + 3, & x^2 + c = 8n + 4, & x^2 - c = 8n + 6 \\ c = 8n + 5, & x^2 + c = 8n + 6, & x^2 - c = 8n + 4 \\ c = 8n + 7, & x^2 + c = 8n \quad , & x^2 - c = 8n + 2. \end{array}$$

Scheidet man demnach die Fälle aus, welche nicht gestatten, dafs $x^2 \pm c$ durch eine höhere Potenz von 2 als die erste teilbar ist, so sind die übrigbleibenden Fälle die folgenden vier:

$$\begin{array}{ll} c = 8n + 1 \quad , & x^2 - c = 8n \\ c = 8n + 3 \quad , & x^2 + c = 8n + 4 \\ c = 8n + 5 \quad , & x^2 - c = 8n + 4 \\ c = 8n + 7 \quad , & x^2 + c = 8n. \end{array}$$

Der zweite und dritte Fall sind nur für den einen Wert $m = 2$ auflösbar, und zwar ist dann die Lösung einfach $x = 1$.

Die beiden andern Fälle, in denen $a = -1 \pm 8\alpha$ ist, sind für beliebige Werte des Exponenten m auflösbar, und kann man zur Lösung leicht durch aufeinanderfolgende Substitutionen gelangen. Ist z. B. die zum vierten Falle gehörige Gleichung

$$\frac{x^2 + 15}{2^{10}} = y$$

gegeben, und setzt man $x = 1$, so hat man $x^2 + 15 = 2^4$. Ist also:

$$x = 1 + 2^3 x',$$



so ergiebt sich durch Substitution die Gleichung:

$$1 + x' + 2^2 x'^2 = 2^6 y.$$

Dieselbe zeigt, dafs $1 + x'$ durch 4 teilbar sein mufs. Setzt man also

$$x' = -1 + 4x'',$$

so erhält man:

$$\frac{1 - 7x''}{16} = e.$$

Folglich: $x'' = 7$, $x' = 27$, $x = 217$.

Sobald man eine specielle Lösung $x = \vartheta$ kennt, so erhält man daraus die allgemeine Lösung $x = 2^{m-1}x' \pm \vartheta$, welche der gegebenen Gleichung $x^2 + a = 2^m y$ genügt, weil $m > 1$ ist. Dieser Wert mufs sodann mit denjenigen verbunden werden, welche ausdrücken, dafs $x^2 + a$ durch die verschiedenen ungeraden Faktoren von N teilbar ist.

Wir haben jetzt zu untersuchen, wieviele Lösungen die Gleichung $\frac{x^2 + a}{N} = e$ haben kann. Jedoch beschränken wir uns hierbei auf die Fälle, wo N eine ungerade Zahl oder das Doppelte einer ungeraden Zahl ist.

192.

Ist N ungerade und prim zu a, so ist die Anzahl der Lösungen der Gleichung

$$\frac{x^2 + a}{N} = e$$

gleich 2^{i-1}, wo i die Anzahl der verschiedenen in N aufgehenden Primfaktoren ist.

Ist zuerst $N = \alpha^\lambda$, wo α eine Primzahl ist, so behaupte ich, dafs es nur eine Weise giebt, der Gleichung $\frac{x^2 + a}{N} = e$ zu genügen. Denn gäbe es zwei Lösungen, welche durch x und x' bezeichnet seien, so müfste $x^2 - x'^2$ durch α^λ teilbar sein, und da keiner der Faktoren $x + x'$, $x - x'$ durch α^λ teilbar ist, weil x und x' als ungleich und kleiner als $\frac{1}{2}\alpha^\lambda$ vorausgesetzt sind, so müssen diese Faktoren $x + x'$, $x - x'$ alle beide durch α teilbar sein. Mithin würde auch ihre Summe $2x$ durch α teilbar sein. Ist aber x durch α teilbar, so müfste der Gleichung $\frac{x^2 + a}{\alpha^\lambda} = e$ zufolge auch a durch α teilbar sein. Da nun a und N prim zu einander sind, so kann die Gleichung $\frac{x^2 + a}{\alpha^\lambda} = e$ nur eine Lösung haben, die kleiner als $\frac{1}{2}\alpha^\lambda$ ist.

Ist zweitens $N = \alpha^\lambda \beta^\mu$ und sind A und B die Werte von x,

welche den Gleichungen $\frac{x^2 + a}{\alpha^\lambda} = e$, $\frac{x^2 + a}{\beta^\mu} = e$ genügen, und kombiniert man ferner nach No. 13 die beiden Werte $x = A + \alpha^\lambda y$ und $y = \pm B + \beta^\mu z$ mit einander, so ist klar, dafs man wegen des doppelten Zeichens $\pm$ zwei Werte von x von der Form

$$x = K + \alpha^\lambda \beta^\mu x' = K + Nx'$$

erhält, von denen jeder dadurch, dafs man für x' den passenden Wert nimmt, kleiner gemacht werden kann als $\frac{1}{2}N$. Mithin hat im Falle zweier ungleichen Faktoren α und β die gegebene Gleichung zwei Lösungen.

Giebt es einen dritten Faktor γ^ν, so mufs man den gefundenen Wert $x = K + \alpha^\lambda \beta^\mu x'$ mit einer dritten Formel $x = \pm C + \gamma^\nu z$ kombinieren, und es ist klar, dafs man vier Lösungen von der Form $K' + \alpha^\lambda \beta^\mu \gamma^\nu x''$ oder $K' + Nx''$ erhält, welche kleiner gemacht werden können als $\frac{1}{2}N$.

Überhaupt verdoppelt jeder neue Faktor die Anzahl der durch die vorhergehenden Faktoren erhaltenen Lösungen. Demnach erhält man 2^{i-1} Lösungen, wenn i die Anzahl der Faktoren α^λ, β^μ, γ^ν, ..., aus denen N zusammengesetzt ist, bezeichnet.

Bemerkung. Ist N das Doppelte einer ungeraden Zahl, so hat die Gleichung $\frac{x^2 + a}{N} = e$ ebenfalls 2^{i-1} Lösungen. Denn ist ϑ ein Wert von x, für welchen $x^2 + a$ durch $\frac{1}{2}N$ teilbar ist, so wird $x^2 + a$ für diesen Wert oder wenigstens für den Wert $\frac{1}{2}N - \vartheta$ durch N teilbar sein.

193.

Ist N eine ungerade Zahl oder das Doppelte einer solchen und haben die beiden Zahlen N und a einen gemeinschaftlichen Teiler ω, welcher durch keine Quadratzahl teilbar ist, so besitzt die Gleichung

$$\frac{x^2 + a}{N} = e$$

stets 2^{i-1} Lösungen, wenn i die Anzahl der ungeraden und ungleichen Primfaktoren ist, welche in N aber nicht in a aufgehen.

Ist nämlich:

$$N = \omega N', \quad a = \omega a', \quad x = \omega x',$$

so geht die gegebene Gleichung über in:

$$\frac{\omega x'^2 + a'}{N'} = e.$$

Da nun ω und N' keinen gemeinsamen Teiler haben, so kann man

$$f\omega - gN' = 1$$

setzen. Dies ergiebt die reducierte Gleichung:

$$\frac{x'^2 + fa'}{N'} = e.$$

Nun besitzt diese, da N' und fa' prim zu einander sind, soviel Lösungen, als in 2^{i-1} Einheiten enthalten sind, wobei i die Anzahl der ungeraden und ungleichen in N' aufgehenden Primfaktoren bezeichnet, und setzt man allgemein:

$$x' = \vartheta + N'x'',$$

so erhält man:

$$x = \omega\vartheta + \omega N'x'' = \omega\vartheta + Nx''.$$

Demnach giebt es ebensoviele Werte von x, die kleiner als $\frac{1}{2}N$ sind, als es Werte von x' giebt, die kleiner als $\frac{1}{2}N'$ sind; mithin ist die Anzahl dieser Werte gleich 2^{i-1}.

194.

Wenn die Zahl N, welche ungerade oder das Doppelte einer ungeraden Zahl ist, mit a einen beliebigen gemeinschaftlichen Teiler hat, und dieser Teiler durch $\omega\psi^2$ dargestellt wird, so dafs $N = \psi^2\omega N'$ ist, wo ω durch kein Quadrat mehr teilbar sein soll, so besitzt die Gleichung

$$\frac{x^2 + a}{N} = e$$

ebenso viele Lösungen, als $\psi \,.\, 2^{i-1}$ Einheiten besitzt, wobei i die Anzahl der ungeraden und ungleichen, in N' aufgehenden Primfaktoren bezeichnet.

In diesem Falle ist nämlich:

$$a = \psi^2\omega a', \quad x = \psi\omega x',$$

und die aufzulösende Gleichung geht über in:

$$\frac{\omega x'^2 + a'}{N'} = e.$$

Dieselbe ergiebt, wie wir in der vorigen Nummer gesehen haben, 2^{i-1} Werte von x', welche kleiner als $\frac{1}{2}N'$ sind. Ist daher allgemein:

$$x' = \vartheta + N'x'',$$

so erhält man:

$$x = \psi\omega\vartheta + \psi\omega N'x''.$$

Da es nun ausreicht, wenn die Werte von x kleiner oder nicht gröfser

als $\frac{1}{2}N = \frac{1}{2}\psi^2 \omega N'$ sind, so kann man offenbar x'' die aufeinanderfolgenden Werte $0, \pm 1, \pm 2, \ldots$ bis $\pm \frac{1}{2}(\psi - 1)$ geben. Die Anzahl dieser Werte ist augenscheinlich gleich ψ. Demnach liefert jeder Wert von x', welcher kleiner als $\frac{1}{2}N'$ ist, ψ Werte von x, welche kleiner sind als $\frac{1}{2}N$. Mithin ist die Anzahl aller Werte von x gleich $\psi \,.\, 2^{i-1}$.

Bemerkung. Diese Formel ist auch für den Fall $i = 0$ richtig, d. h. wenn die Zahl N oder wenigstens die Hälfte derselben ein Teiler von a ist. Alsdann reduciert sie sich auf $\frac{1}{2}\psi$; man mufs jedoch den in $\frac{1}{2}\psi$ enthaltenen Bruch als ganz rechnen, so dafs, wenn $\psi = 2h + 1$ ist, man $h + 1$ für $\frac{1}{2}\psi$ zu nehmen hat.

§ 9.

Auflösung der symbolischen Gleichungen $\left(\frac{x}{c}\right) = 1$, $\left(\frac{x}{c}\right) = -1$, in denen c eine Primzahl ist.

195.

Es sei c irgend eine Primzahl, und es sei die Aufgabe gestellt, alle Werte von x zu finden, welche der Gleichung

$$\left(\frac{x}{c}\right) = 1 \quad \text{oder} \quad \frac{x^{\frac{c-1}{2}} - 1}{c} = e$$

genügen.

Wie leicht zu sehen, kann man $x = y^2$ setzen, wo y irgend eine durch c nicht teilbare Zahl ist. Demnach werden die verschiedenen Werte von x sein:

$$1, 4, 9, 16, \ldots \text{ bis } \left(\frac{c-1}{2}\right)^2 \text{ einschliefslich.}$$

Diese Werte können sämtlich unter c herabgedrückt werden, wenn man davon die in ihnen enthaltenen Vielfachen von c subtrahiert, und ihre Anzahl ist, wie man sieht, $\frac{c-1}{2}$. Sie kann nicht gröfser sein, da der Exponent von x nur $\frac{c-1}{2}$ ist; sie kann aber auch nicht kleiner sein, da, wenn die beiden Quadrate m^2, n^2, von denen jedes kleiner als $\left(\frac{c-1}{2}\right)^2$ ist, denselben Rest oder denselben Wert von x ergäben, $m^2 - n^2$ durch c teilbar sein müfste. Dies kann jedoch

nicht der Fall sein, da $m + n$ und $m - n$ alle beide kleiner als c sind. Wir kennen also die $\frac{c-1}{2}$ Lösungen der Gleichung $\left(\frac{x}{c}\right) = 1$, wenn diese Lösungen zwischen 0 und c liegen. Da es sich jedoch nur um ungeradzahlige Lösungen handelt, so wird man von den Werten von x die ungeraden Zahlen beibehalten und zu den geraden Zahlen c addieren, was ebenfalls $\frac{c-1}{2}$ ungeradzahlige, zwischen 1 und $2c - 1$ enthaltene Lösungen ergiebt.

Um unmittelbar zu diesen Lösungen zu gelangen, bilde man mit Hülfe der Differenzen die Reihe der ungeraden Quadrate, wie im Folgenden:

Differenzen: 8, 16, 24, 32, 40, 48, 56

Quadrate: 1, 9, 25, 49, 81, 121, 169, 225, ...,

und ziehe sowohl bei den Differenzen wie bei den Quadraten die Vielfachen von $2c$ ab, so oft sie vorkommen, so wird die Reihe der Quadrate oder vielmehr die Reihe ihrer Reste, bis zu $\frac{c-1}{2}$ Gliedern fortgesetzt, alle Lösungen der Gleichung $\left(\frac{x}{c}\right) = 1$ enthalten, welche ungerade, positiv und kleiner als $2c$ sind. Darauf kann man diese Lösungen um irgend ein Vielfaches von $2c$ vermehren; dies giebt $x = 2cz + b$, wo b $\frac{c-1}{2}$ verschiedene Werte hat.

Wenn man auf diese Weise alle Lösungen der Gleichung $\left(\frac{x}{c}\right) = 1$ kennt, so findet man auch, indem man diese ausscheidet, sämtliche Lösungen der Gleichung $\left(\frac{x}{c}\right) = -1$. Denn diejenigen Zahlen, welche kleiner als $2c$ und nicht unter den Lösungen der Gleichung $\left(\frac{x}{c}\right) = 1$ enthalten sind, genügen notwendig der Gleichung $\left(\frac{x}{c}\right) = -1$. Die Anzahl dieser letzteren ist ebenfalls $\frac{c-1}{2}$; denn da die Anzahl der Glieder der Progression $1, 3, 5, 7, \ldots 2c - 1$ gleich c ist, so bleiben, wenn man das Glied c, welches weder der einen noch der andern von diesen Gleichungen genügt, ausschliefst, $c - 1$ Glieder übrig, von denen die eine Hälfte der Gleichung $\left(\frac{x}{c}\right) = 1$, die andere Hälfte der Gleichung $\left(\frac{x}{c}\right) = -1$ genügt. Es braucht wohl nicht erst hinzugefügt zu werden, dafs man die Lösungen dieser letzteren Gleichung ebenfalls um irgend ein Vielfaches von $2c$ vermehren kann.

196.

Beispiel 1.

Ist $c = 41$, so bilde man mit Hülfe der Differenzen die Reihe der ungeraden Quadrate, und ziehe sowohl von den Differenzen wie von den Quadraten die Vielfachen von 82, so oft solche vorkommen, ab. Die Rechnung ist folgende:

Differenzen: 8, 16, 24, 32, 40, 48, 56, 64, 72,
Quadrate: 1, 9, 25, 49, 81, 121 = 39, 87 = 5, 61, 125 = 43,
Differenzen: 80, 88 = 6, 14, 22, 30, 38, 46,
Quadrate: 115 = 33, 113 = 31, 37, 51, 73, 103 = 21, 59,
Differenzen: 54, 62, 70, 78, 86 = 4
Quadrate: 105 = 23, 77, 139 = 57, 127 = 45, 123 = 41 = c.

Die zwanzig ersten Glieder geben, nach ihrer Gröfse geordnet, die folgende Formel, welche alle Lösungen der Gleichung $\left(\frac{x}{41}\right) = 1$ enthält:

$$x = 82z + \begin{cases} 1, & 5, & 9, & 21, & 23, & 25, & 31, & 33, & 37, & 39, \\ 81, & 77, & 73, & 61, & 59, & 57, & 51, & 49, & 45, & 43. \end{cases}$$

Man beachte, dafs die zwanzig Zahlwerte, welche hinter $82z$ stehen, und die eigentlich die Lösungen der gegebenen Gleichung sind, derart sind, dafs jeder Wert von b zusammen mit seinem Komplement $2c - b$ vorkommt, so dafs beide zusammen beständig $2c$ ergeben. Dies ist allgemein immer dann der Fall, wenn die Zahl c von der Form $4m + 1$ ist; denn ist $b^{2m} - 1$ durch c teilbar, so ist offenbar $(2c - b)^{2m} - 1$ ebenfalls durch c teilbar. Mithin kommt alsdann die Lösung oder Wurzel b stets mit der Wurzel $2c - b$ zusammen vor. Dies würde aber nicht stattfinden, wenn c von der Form $4m + 3$ wäre; vielmehr sieht man, dafs, wenn b der Gleichung $\left(\frac{x}{c}\right) = 1$ genügt, sein Komplement $2c - b$ der Gleichung $\left(\frac{x}{c}\right) = -1$ Genüge leistet.

197.

Beispiel 2.

Ist $c = 59$, $2c = 118$, so verfahre man folgendermafsen:

Differenzen: 8, 16, 24, 32, 40, 48, 56, 64, 72,
Quadrate: 1, 9, 25, 49, 81, 121 = 3, 51, 107, 171 = 53,

Differenzen: 80, 88, 96, 104, 112, 120 = 2, 10,
Quadrate: 125 = 7, 87, 175 = 57, 153 = 35, 139 = 21, 133 = 15, 17,

Differenzen: 18, 26, 34, 42, 50, 58, 66, 74, 82,
Quadrate: 27, 45, 71, 105, 147 = 29, 79, 137 = 19, 85, 159 = 41,

Differenzen: 90, 98, 106, 114
Quadrate: 123 = 5, 95, 193 = 75, 181 = 63.

Ordnet man wieder diese 29 Resultate nach der Gröfse, so erhält man die folgende Formel, welche sämtliche Lösungen der Gleichung $\left(\frac{x}{59}\right) = 1$ enthält:

$x = 118z + 1, 3, 5, 7, 9;\ 15, 17, 19, 21, 25;\ 27, 29, 35, 41, 45;$
$49, 51, 53, 57, 63;\ 71, 75, 79, 81, 85;\ 87, 95, 105, 107.$

Mithin sind die Lösungen der Gleichung $\left(\frac{x}{59}\right) = -1$ die folgenden:

$x = 118z + 11, 13, 23, 31, 33;\ 37, 39, 43, 47, 55;\ 61, 65, 67, 69,$
$73;\ 77, 83, 89, 91, 93;\ 97, 99, 101, 103, 109;\ 111,$
$113, 115, 117.$

§ 10.

Ermittlung der linearen Formen, welche den Teilern der Formel $t^2 + cu^2$ zukommen.

Wir werden zunächst den Fall untersuchen, wo c eine Primzahl ist. Für diesen ergeben sich zwei Hauptsätze:

198.

Satz. Ist c eine Primzahl $4n + 1$ und A ein beliebiger ungerader Teiler der Formel $x^2 + c$ oder $t^2 + cu^2$, so ist $\left(\frac{A}{c}\right) = 1$, wenn A von der Form $4n + 1$, und $\left(\frac{A}{c}\right) = -1$, wenn A von der Form $4n + 3$ ist.

Denn ist α eine Primzahl von der Form $4n + 1$ und β eine Primzahl von der Form $4n + 3$, welche beide Teiler von $x^2 + c$ sind, so hat man nach No. 134:

$$\left(\frac{-c}{\alpha}\right) = 1 \quad \text{und} \quad \left(\frac{-c}{\beta}\right) = 1,$$

oder:

$$\left(\frac{c}{\alpha}\right) = 1 \quad \text{und} \quad \left(\frac{c}{\beta}\right) = -1.$$

Hieraus folgt nach dem Reciprocitätsgesetz:

$$\left(\frac{\alpha}{c}\right) = 1 \quad \text{und} \quad \left(\frac{\beta}{c}\right) = -1.$$

Nun ist aber die Zahl A, falls sie von der Form $4n + 1$ ist, das Produkt einer beliebigen Anzahl von Faktoren α und einer geraden Anzahl von Faktoren β; mithin ist in diesem Falle $\left(\frac{A}{c}\right) = +1$. Ist dagegen die Zahl A von der Form $4n + 3$, so entsteht sie durch Multiplikation einer beliebigen Anzahl von Faktoren α mit einer ungeraden Anzahl von Faktoren β; mithin ist in diesem zweiten Falle $\left(\frac{A}{c}\right) = -1$.

Zusatz. Bezeichnet man also mit b eine der $\frac{c-1}{2}$ ungeraden Zahlen, welche kleiner als $2c$ sind und der Gleichung $\left(\frac{x}{c}\right) = 1$ genügen, so hat man $A = 2cz + b$. Von den Zahlen b kann man diejenigen, welche von der Form $4n + 1$ sind, beibehalten und zu denen, welche von der Form $4n + 3$ sind, $2c$ addieren. Dadurch erhält man $\frac{c-1}{2}$ Zahlen von der Form $4n + 1$, welche kleiner sind als $4c$. Ist a eine dieser Zahlen, so ist $A = 4cz + a$. Dies giebt $\frac{c-1}{2}$ **lineare Formen** für die Teiler der Formel $t^2 + cu^2$, welche von der Form $4n + 1$ sind.

Wenn man in gleicher Weise alle Lösungen der Gleichung $\left(\frac{x}{c}\right) = -1$ auf die Form $4n + 3$ bringt, was dadurch geschieht, daſs man die Zahlen von der Form $4n + 3$ beibehält und zu denen von der Form $4n + 1$ $2c$ addiert, so erhält man $\frac{c-1}{2}$ Zahlen von der Form $4n + 3$, die kleiner sind als $4c$. Ist a irgend eine dieser Zahlen, so ist der Ausdruck $4cz + a$ die allgemeine Form für die Teiler $4n + 3$ der Formel $t^2 + cu^2$.

So sind z. B. die Teiler $4n + 1$ der Formel $t^2 + 41u^2$ in der Formel enthalten:

$A = 164z + 1$, 5, 9, 21, 25; 33, 37, 45, 49, 57; 61, 73, 77, 81, 105; 113, 121, 125, 133, 141,

und die Teiler $4n + 3$ derselben Formel sind enthalten in:

$A = 164z + 3$, 7, 11, 15, 19; 27, 35, 47, 55, 63; 67, 71, 75, 79, 95; 99, 111, 135, 147, 151.

Durch Ausscheidung dieser ergeben sich die verschiedenen Formen, welche nicht in $t^2 + 41u^2$ aufgehen und entweder von der Form

$4n+1$ oder von der Form $4n+3$ sind. Überhaupt erkennt man leicht, dafs es stets ebensoviele Formen für die Nichtteiler wie für die Teiler giebt, und zwar ist ihre Anzahl gleich $\frac{c-1}{2}$ sowohl bei der Form $4n+1$ wie bei der Form $4n+3$.

Bemerkung. Jede in den linearen Formen der Teiler von t^2+cu^2 enthaltene Primzahl ist notwendig ein Teiler von t^2+cu^2. Denn ist A diese Primzahl, so hat man, falls sie von der Form $4n+1$ ist, $\left(\frac{A}{c}\right)=1$, mithin $\left(\frac{c}{A}\right)=1$, folglich A ein Teiler von t^2+cu^2. Ist aber A von der Form $4n+3$, so hat man $\left(\frac{A}{c}\right)=-1$, mithin $\left(\frac{c}{A}\right)=-1$, folglich A ein Teiler von t^2+cu^2.

Auf dieser Bemerkung beruht eine grofse Anzahl von Eigenschaften der Primzahlen. Denn da man für ein gegebenes c a priori alle linearen Formen $4cz+b$, welche die Teiler der Formel t^2+cu^2 annehmen können, bestimmen kann, und da man andererseits auch alle quadratischen Formen $py^2+2qyz+rz^2$, welche eben diesen Teilern zukommen, zu bestimmen imstande ist, so folgt daraus, dafs jede in einer der linearen Formen

$$4cz+b$$

enthaltene Primzahl von einer der quadratischen Formen

$$py^2+2qyz+rz^2$$

sein mufs. Es ist dies ein äufserst fruchtbarer Satz, dessen nähere Entwicklung für die verschiedenen Werte der Primzahl c eine Menge interessanter Sätze über die Primzahlen liefert.

Ist A eine zusammengesetzte Zahl, so genügt es nicht, dafs dieselbe in den Formen $4cz+b$, welche den Teilern von t^2+cu^2 zukommen, enthalten sei; denn trotz dieser Bedingung könnte es vorkommen, dafs A kein Teiler dieser Formel ist. Ist z. B. $c=41$, so enthält die Form $164z+57$ die Zahl $221=13.17$, welche kein Teiler von t^2+41u^2 ist, da weder 13 noch 17 in t^2+41u^2 aufgeht.

199.

Satz. Ist c eine Primzahl von der Form $4n+3$ und A irgend ein ungerader Teiler der Formel t^2+cu^2, so hat man stets $\left(\frac{A}{c}\right)=1$.

Denn ist α eine Primzahl von der Form $4n+1$ und β eine Primzahl von der Form $4n+3$, welche beide Teiler von t^2+cu^2 sind, so hat man:

$$\left(\frac{-c}{\alpha}\right)=1 \quad \text{und} \quad \left(\frac{-c}{\beta}\right)=1,$$

oder:

$$\left(\frac{c}{\alpha}\right) = 1 \quad \text{und} \quad \left(\frac{c}{\beta}\right) = -1.$$

Folglich umgekehrt:

$$\left(\frac{\alpha}{c}\right) = 1 \quad \text{und} \quad \left(\frac{\beta}{c}\right) = 1.$$

Mithin giebt jeder Teiler A, welcher das Produkt von mehreren Primzahlen α und β ist, $\left(\frac{A}{c}\right) = 1$.

Zusatz. Jeder ungerade Teiler der Formel $t^2 + cu^2$ läfst sich darstellen in der Form $2cz + a$, wo a eine der $\frac{c-1}{2}$ ungeraden Zahlen ist, welche kleiner als $2c$ sind und der Gleichung $\left(\frac{x}{c}\right) = 1$ genügen.

So kann z. B., wenn $c = 59$ ist, jeder ungerade Teiler der Formel $t^2 + 59u^2$ dargestellt werden durch die Formel:

$$A = 118z + 1, 3, 5, 7, 9;\ 15, 17, 19, 21, 25;\ 27, 29, 35, 41, 45;\ 49, 51, 53, 57, 63;\ 71, 75, 79, 81, 85;\ 87, 95, 105, 107.$$

Ebenso wie im vorhergehenden Falle beweist man ferner, dafs jede in der linearen Form $2cz + a$ enthaltene Primzahl notwendig ein Teiler von $t^2 + cu^2$ ist.

Bemerkung. Man würde, was die Teiler der Formel $t^2 - cu^2$ anlangt, ebenso die folgenden **Sätze** finden:

1) Ist c eine Primzahl von der Form $4n + 1$ und A ein beliebiger ungerader Teiler der Formel $t^2 - cu^2$, so hat man $\left(\frac{A}{c}\right) = 1$. Mithin ist A immer von der Form $2cz + a$, wo a eine der $\frac{c-1}{2}$ Lösungen der Gleichung $\left(\frac{x}{c}\right) = 1$ ist. Umgekehrt ist jede in den Formen $2cz + a$ enthaltene Primzahl ein Teiler der Formel $t^2 - cu^2$.

2) Ist c eine Primzahl von der Form $4n + 3$ und A ein beliebiger ungerader Teiler der Formel $t^2 - cu^2$, so ist $\left(\frac{A}{c}\right) = 1$, falls A von der Form $4n + 1$, dagegen $\left(\frac{A}{c}\right) = -1$, falls A von der Form $4n + 3$ ist. Daraus ergeben sich leicht die linearen Formen, welche dem Teiler A zukommen. Umgekehrt ist jede in diesen Formen enthaltene Primzahl ein Teiler der Formel $t^2 - cu^2$.



200.

Wir betrachten jetzt die Teiler der Formel $t^2 + 2cu^2$, in welcher c eine Primzahl ist.

Ist zunächst $c = 4n + 1$ und sind a, a', a'', a''' Primzahlen resp. von den Formen $8n + 1$, $8n + 3$, $8n + 5$, $8n + 7$, welche sämtlich Teiler von $t^2 + 2cu^2$ sind, so hat man in diesen verschiedenen Fällen (No. 134):

$$\left(\frac{2c}{a}\right) = 1, \quad \left(\frac{2c}{a'}\right) = -1, \quad \left(\frac{2c}{a''}\right) = 1, \quad \left(\frac{2c}{a'''}\right) = -1.$$

Zugleich aber ist (No. 150):

$$\left(\frac{2}{a}\right) = 1, \quad \left(\frac{2}{a'}\right) = -1, \quad \left(\frac{2}{a''}\right) = -1, \quad \left(\frac{2}{a'''}\right) = 1.$$

Mithin:

$$\left(\frac{c}{a}\right) = 1, \quad \left(\frac{c}{a'}\right) = 1, \quad \left(\frac{c}{a''}\right) = -1, \quad \left(\frac{2}{a'''}\right) = -1.$$

Folglich umgekehrt:

$$\left(\frac{a}{c}\right) = 1, \quad \left(\frac{a'}{c}\right) = 1, \quad \left(\frac{a''}{c}\right) = -1, \quad \left(\frac{a'''}{c}\right) = -1.$$

Es sei jetzt A irgend eine Zahl von einer der beiden Formen $8n + 1$, $8n + 3$, und B eine Zahl von einer der beiden Formen $8n + 5$, $8n + 7$. Alsdann entsteht A notwendig durch Multiplikation einer beliebigen Anzahl von Faktoren a, a' mit einer geraden Anzahl von Faktoren a'', a''', so dafs stets $\left(\frac{A}{c}\right) = 1$ ist. Ebenso entsteht die Zahl B durch Multiplikation einer beliebigen Anzahl von Faktoren a, a' mit einer ungeraden Anzahl von Faktoren a'', a''', so dafs $\left(\frac{B}{c}\right) = -1$ ist.

Ist zweitens $c = 4n + 3$ und sind stets $a, a', \ldots$ Primzahlen von den Formen $8n + 1$, $8n + 3, \ldots$, welche sämtlich Teiler von $t^2 + 2cu^2$ sind, so erhält man, wie oben:

$$\left(\frac{c}{a}\right) = 1, \quad \left(\frac{c}{a'}\right) = 1, \quad \left(\frac{c}{a''}\right) = -1, \quad \left(\frac{c}{a'''}\right) = -1.$$

Demnach umgekehrt:

$$\left(\frac{a}{c}\right) = 1, \quad \left(\frac{a'}{c}\right) = -1, \quad \left(\frac{a''}{c}\right) = -1, \quad \left(\frac{a'''}{c}\right) = 1.$$

Sind nun A und B zwei zusammengesetzte Zahlen, erstere von der Form $8n + 1$ oder $8n + 7$, letztere von der Form $8n + 3$ oder $8n + 5$, so ist leicht zu sehen, dafs die Zahl A durch Multiplikation

einer beliebigen Anzahl von Faktoren a, a''' mit einer geraden Anzahl von Faktoren a', a'' entsteht, und demnach stets $\left(\frac{A}{c}\right) = 1$ ist. Was die Zahl B angeht, so kann dieselbe als Produkt aus einer Zahl A und einem der Faktoren a', a'' betrachtet werden; es ist daher $\left(\frac{B}{c}\right) = -1$.

Wir können daher folgende beiden Sätze aufstellen:

I. Ist A ein beliebiger Teiler der Formel $t^2 + 2cu^2$ von der Form $8n + 1$ oder $8n + 3$ und B ein Teiler derselben Formel von der Form $8n + 5$ oder $8n + 7$, so erhält man, wenn c eine Primzahl von der Form $4n + 1$ ist, stets $\left(\frac{A}{c}\right) = 1$ und $\left(\frac{B}{c}\right) = -1$.

II. Ist A ein Teiler der Formel $t^2 + 2cu^2$ von der Form $8n + 1$ oder $8n + 7$ und B ein Teiler derselben Formel von der Form $8n + 3$ oder $8n + 5$, so erhält man, wenn c eine Primzahl von der Form $4n + 3$ ist, stets $\left(\frac{A}{c}\right) = 1$ und $\left(\frac{B}{c}\right) = -1$.

201.

Man ersieht hieraus, dafs man a priori alle linearen Formen $8cx + b$, welche den Teilern A wie den Teilern B der Formel $t^2 + 2cu^2$ zukommen, bestimmen kann.

Ist z. B. $c = 29$, so sind die Lösungen der Gleichung $\left(\frac{A}{c}\right) = 1$:

$$A = 58z + 1,\ 5,\ 7,\ 9,\ 13;\ 23,\ 25,\ 33,\ 35,\ 45;\ 49,\ 51,\ 53,\ 57.$$

Bringt man diese Lösungen mit den Formen $8n + 1$, $8n + 3$ in Übereinstimmung, so erhält man alle Formen der Teiler der Formel $t^2 + 58u^2$ von der Form $8n + 1$ und $8n + 3$, nämlich:

$$A = 232z + 1,\ 9,\ 25,\ 33,\ 35;\ 49,\ 51,\ 57,\ 59,\ 65;\ 67,\ 81,\ 83,\ 91,\ 107;\ 115,\ 121,\ 123,\ 129,\ 139;\ 161,\ 169,\ 179,\ 187,\ 209;\ 219,\ 225,\ 227.$$

Ebenso findet man für dieselbe Formel sämtliche Teiler von der Form $8n + 5$ und $8n + 7$, nämlich:

$$B = 232z + 15,\ 21,\ 31,\ 37,\ 39;\ 47,\ 55,\ 61,\ 69,\ 77;\ 79,\ 85,\ 95,\ 101,\ 119;\ 127,\ 133,\ 135,\ 143,\ 157;\ 159,\ 189,\ 191,\ 205,\ 213;\ 215,\ 221,\ 229.$$



Ist ferner $c = 11$, so besitzt die Gleichung $\left(\frac{x}{11}\right) = 1$ die Lösungen:

$$x = 22z + 1,\ 3,\ 5,\ 9,\ 15.$$

Bringt man jede Lösung auf die Formen $8n + 1$ und $8n + 7$, so erhält man für die Formel $t^2 + 22u^2$ alle Formen der Teiler von der Form $8n + 1$ und $8n + 7$, nämlich:

$$A = 88z + 1,\ 9,\ 15,\ 23,\ 25;\ 31,\ 47,\ 49,\ 71,\ 81.$$

Ebenso besitzt die Gleichung $\left(\frac{x}{11}\right) = -1$ die Lösungen:

$$x = 22z + 7,\ 13,\ 17,\ 19,\ 21.$$

Bringt man dieselben auf die Formen $8n + 3$, $8n + 5$, so erhält man für die Formel $t^2 + 22u^2$ sämtliche Formen der Teiler von der Form $8n + 3$ und $8n + 5$, nämlich:

$$B = 88z + 13,\ 19,\ 21,\ 29,\ 35;\ 43,\ 51,\ 61,\ 83,\ 85.$$

202.

Nachdem wir so die verschiedenen linearen Formen $8cx + b$, welche den Teilern der Formel $t^2 + 2cu^2$ zukommen, bestimmt haben, können wir beweisen, dafs jede in diesen Formen enthaltene Primzahl notwendig ein Teiler von $t^2 + 2cu^2$ ist. Denn ist z. B. A von der Form $8n + 3$ und c von der Form $4n + 1$, so hat man (No. 200): $\left(\frac{A}{c}\right) = 1$, und daher $\left(\frac{c}{A}\right) = 1$. Ferner ist wegen der Form der Zahl A: $\left(\frac{2}{A}\right) = -1$, also $\left(\frac{-2c}{A}\right) = 1$; mithin ist A ein Teiler von $t^2 + 2cu^2$. Die andern Fälle werden in derselben Weise bewiesen.

Bemerkung. Es ist wesentlich zu bemerken, dafs, mag die Zahl c beschaffen sein, wie sie will, ob Primzahl oder nicht, ob positiv oder negativ, die linearen Teiler der Formel $t^2 + cu^2$ dieselben sind, mögen nun diese Teiler als Primzahlen vorausgesetzt werden, oder mögen sie beliebige zusammengesetzte Zahlen sein.

Betrachtet man nämlich unter den Teilern der Formel $t^2 + cu^2$ nur diejenigen, welche prim zu c sind (und es ist unnötig, andere zu betrachten, weil man weifs, dafs jeder Teiler von c in der Formel $t^2 + cu^2$ aufgeht), und stellt man durch $2cz + b$ einen der betreffenden linearen Teiler dar, so wird b prim zu c sein, so dafs die Formel $2cz + b$ notwendig Primzahlen und sogar in unendlicher Anzahl enthält (siehe weiter unten Hauptteil IV). Demnach ist die Form

$2cz + b$ unter allen möglichen Formen der Primzahlen, welche Teiler der Formel $t^2 + cu^2$ sind, enthalten. Man braucht daher nur alle linearen Formen der Primzahlen zu suchen; dieselben werden absolut alle möglichen Formen sowohl der einfachen wie der zusammengesetzten Teiler enthalten.

Diese Bemerkung kürzt die Rechnungen, welche erforderlich sind, um die linearen Formen der Teiler der Formel $t^2 + cu^2$, wo c eine zusammengesetzte Zahl ist, a priori zu bestimmen, aufserordentlich ab. Wir werden diese Methode auf einige allgemeine Fälle anwenden; sodann werden wir eine andere Methode angeben, die zwar weniger direkt ist, aber bedeutend schneller zum Ziele führt.

203.

Aufgabe. Ist $c = \alpha\beta$, wo α und β irgend welche Primzahlen aufser 2 sind, so verlangt man zu wissen, welche Form die Primzahl A besitzen müsse, damit A in der Formel $t^2 + \alpha\beta u^2$ aufgehe.

Allgemein mufs $\left(\frac{-\alpha\beta}{A}\right) = 1$ sein. Um aber dieser Gleichung zu genügen, unterscheiden wir zwei Fälle, je nachdem A von der Form $4n + 1$ oder von der Form $4n + 3$ ist.

1) Ist A eine Primzahl von der Form $4n + 1$, so ist die aufzulösende Gleichung:

$$\left(\frac{\alpha}{A}\right)\left(\frac{\beta}{A}\right) = 1.$$

Derselben kann man nur auf zwei Arten genügen, nämlich einmal, indem man setzt:

$$\left(\frac{\alpha}{A}\right) = 1, \qquad \left(\frac{\beta}{A}\right) = 1,$$

das andre Mal, indem man setzt:

$$\left(\frac{\alpha}{A}\right) = -1, \quad \left(\frac{\beta}{A}\right) = -1.$$

In dem ersten Falle hat man nach dem Reciprocitätsgesetz:

$$\left(\frac{A}{\alpha}\right) = 1, \qquad \left(\frac{A}{\beta}\right) = 1.$$

Ist die erste Gleichung nach dem oben entwickelten Verfahren gelöst, und sind die Lösungen sämtlich auf die Form $4n + 1$ gebracht, so hat man $\frac{\alpha - 1}{2}$ Werte von A von der Form $4\alpha z + \alpha'$. Ebenso liefert die zweite Gleichung $\frac{\beta - 1}{2}$ Werte von A von der Form $4\beta z + \beta'$.

Bringt man also jede der Formeln $4\alpha z + \alpha'$ in Übereinstimmung mit jeder der Formeln $4\beta z + \beta'$, so erhält man im Ganzen $\frac{\alpha-1}{2}\cdot\frac{\beta-1}{2}$ Formeln von folgender Art: $A = 4\alpha\beta z + \gamma$.

Im zweiten Falle erhält man analog die Gleichungen:

$$\left(\frac{A}{\alpha}\right) = -1, \quad \left(\frac{A}{\beta}\right) = -1.$$

Werden dieselben zuerst jede für sich gelöst, und kombiniert man darnach ihre Lösungen mit einander, so ergeben sich ebenso $\frac{\alpha-1}{2}\cdot\frac{\beta-1}{2}$ Formeln von der Form $A = 4\alpha\beta z + \gamma$.

2) Ist A eine Primzahl von der Form $4n + 3$, so ist die Bedingung zu erfüllen:

$$\left(\frac{\alpha\beta}{A}\right) = -1 \qquad \text{oder} \qquad \left(\frac{\alpha}{A}\right)\cdot\left(\frac{\beta}{A}\right) = -1.$$

Man kann derselben nur auf zwei Arten genügen; entweder indem man setzt:

$$\left(\frac{\alpha}{A}\right) = 1, \qquad \left(\frac{\beta}{A}\right) = -1,$$

oder indem man setzt:

$$\left(\frac{\alpha}{A}\right) = -1, \quad \left(\frac{\beta}{A}\right) = 1.$$

Die zweite Art giebt dem Reciprocitätsgesetz zufolge (No. 166):

$$\left(\frac{A}{\alpha}\right) = (-1)^{\frac{\alpha+1}{2}}, \qquad \left(\frac{A}{\beta}\right) = (-1)^{\frac{\beta-1}{2}}.$$

Da diese Gleichungen stets mit einer der beiden Gleichungen

$$\left(\frac{x}{c}\right) = +1, \quad \left(\frac{x}{c}\right) = -1,$$

in denen c eine Primzahl ist, übereinstimmen, so kann man leicht den Wert von A erhalten, welcher jeder von diesen Gleichungen genügt. Sodann giebt die Kombination der Werte $\frac{\alpha-1}{2}\cdot\frac{\beta-1}{2}$ Lösungen, welche sämtlich von der Form $4\alpha\beta z + a$ sind.

Die erste Art, der Aufgabe zu genügen, giebt:

$$\left(\frac{A}{\alpha}\right) = (-1)^{\frac{\alpha-1}{2}}, \qquad \left(\frac{A}{\beta}\right) = (-1)^{\frac{\beta+1}{2}}.$$

Hieraus zieht man ähnliche Folgerungen. Es giebt daher im Ganzen vier allgemeine Formeln $4\alpha\beta z + a$, von denen jede $\frac{\alpha-1}{2}\cdot\frac{\beta-1}{2}$ Werte für a enthält.

204.

Setzt man $c = \alpha\beta\gamma$ voraus, wo α, β, γ drei ungleiche Primzahlen aufser 2 sind, so verfährt man, um die Form der verschiedenen Primzahlen, welche Teiler der Formel $t^2 + cu^2$ sind, zu finden, in ähnlicher Weise.

Ist A eine dieser Zahlen, so mufs man allgemein haben:

$$\left(\frac{-\alpha\beta\gamma}{A}\right) = 1.$$

Nehmen wir zunächst an, dafs A von der Form $4n + 1$ sei, so wird diese Gleichung:

$$\left(\frac{\alpha}{A}\right)\left(\frac{\beta}{A}\right)\left(\frac{\gamma}{A}\right) = 1,$$

und dieser kann man nur auf folgende vier Arten Genüge leisten:

1) $\left(\frac{\alpha}{A}\right) = 1, \quad \left(\frac{\beta}{A}\right) = 1, \quad \left(\frac{\gamma}{A}\right) = 1;$

2) $\left(\frac{\alpha}{A}\right) = 1, \quad \left(\frac{\beta}{A}\right) = -1, \quad \left(\frac{\gamma}{A}\right) = -1;$

3) $\left(\frac{\alpha}{A}\right) = -1, \quad \left(\frac{\beta}{A}\right) = 1, \quad \left(\frac{\gamma}{A}\right) = -1;$

4) $\left(\frac{\alpha}{A}\right) = -1, \quad \left(\frac{\beta}{A}\right) = -1, \quad \left(\frac{\gamma}{A}\right) = 1.$

Im ersten Falle erhält man nach dem Reciprocitätsgesetz:

$$\left(\frac{A}{\alpha}\right) = 1, \quad \left(\frac{A}{\beta}\right) = 1, \quad \left(\frac{A}{\gamma}\right) = 1.$$

Nun sind die Werte, welche diesen Gleichungen genügen, von der Form:

$$A = 4\alpha z + \alpha', \quad A = 4\beta z + \beta', \quad A = 4\gamma z + \gamma',$$

wobei α' $\frac{\alpha - 1}{2}$ Werte kleiner als 4α, β' $\frac{\beta - 1}{2}$ Werte kleiner als 4β und γ' $\frac{\gamma - 1}{2}$ Werte kleiner als 4γ besitzt. Bringt man demnach die drei Werte $4\alpha z + \alpha'$, $4\beta z + \beta'$, $4\gamma z + \gamma'$ in allen möglichen Kombinationen mit einander in Übereinstimmung, so erhält man eine neue Formel $A = 4\alpha\beta\gamma z + a$, in welcher a $\frac{\alpha - 1}{2} \cdot \frac{\beta - 1}{2} \cdot \frac{\gamma - 1}{2}$ Werte besitzt.

Eine ähnliche Formel giebt es in jedem der andern Fälle, die man, wenn A von der Form $4n + 1$ ist, zu betrachten hat. Ferner giebt es vier analoge Formeln, welche die Werte von A in dem

Falle darstellen, wenn A von der Form $4n+3$ ist. Man erhält daher im Ganzen acht Formeln, von denen jede $\frac{\alpha-1}{2}\cdot\frac{\beta-1}{2}\cdot\frac{\gamma-1}{2}$ verschiedene Formen unter sich begreift.

Es ist nicht schwer zu sehen, dafs, wenn c einen vierten Faktor δ enthielte, die Anzahl der Formeln doppelt so grofs und die Anzahl der in jeder derselben enthaltenen Formen $\frac{\alpha-1}{2}\cdot\frac{\beta-1}{2}\cdot\frac{\gamma-1}{2}\cdot\frac{\delta-1}{2}$ sein würde. Man kann daher folgenden allgemeinen Schlufs machen:

Bezeichnet man mit m die Anzahl der Primfaktoren $\alpha, \beta, \gamma, \ldots$, aus denen die Zahl c besteht, so sind die ungeraden Teiler der Formel t^2+cu^2 dargestellt durch 2^m Formeln $A=4cz+a$, in deren jeder a eine Anzahl von $\frac{\alpha-1}{2}\cdot\frac{\beta-1}{2}\cdot\frac{\gamma-1}{2}\cdot\frac{\delta-1}{2}\cdots$ Werten besitzt, so dafs die Anzahl aller in diesen Formeln enthaltenen linearen Formen gleich $(\alpha-1)(\beta-1)(\gamma-1)(\delta-1)\ldots$ ist.

Es kann der Fall eintreten, dafs die Formen $4n+1$, $4n+3$ in einer und derselben Formel, welche alsdann $2cz+a$ an Stelle der soeben gefundenen $4cz+a$ sein würde, vereinigt sind; alsdann aber würde es nur halb so viel Formeln geben, was auf dasselbe hinauskäme.

205.

Ist $c=2d$, wo d eine ungerade Zahl und gleich dem Produkte der m Primzahlen $\alpha, \beta, \gamma, \ldots$ ist, so mufs man, was den Teiler A betrifft, die vier Formen $8n+1$, $8n+3$, $8n+5$, $8n+7$ betrachten, deren jede einen bestimmten Wert für $\left(\frac{2}{A}\right)$ liefert, so dafs man je nach den einzelnen Fällen nur noch einer der beiden Gleichungen

$$\left(\frac{d}{A}\right)=1, \qquad \left(\frac{d}{A}\right)=-1$$

zu genügen hat.

Wird diese Gleichung wieder in derselben Weise behandelt, so liefert sie 2^{m-1} Werte von A, jeden von der Form $8dz+a$, wo a eine Anzahl von $\frac{\alpha-1}{2}\cdot\frac{\beta-1}{2}\cdot\frac{\gamma-1}{2}\cdots$ Werten besitzt. Da dasselbe für jede der vier Formen $8n+1$, $8n+3, \ldots$ gilt, so erhält man also im Ganzen 2^{m+1} Formeln $A=8dz+a$, oder $A=4cz+a$, in deren jeder a eine Anzahl von $\frac{\alpha-1}{2}\cdot\frac{\beta-1}{2}\cdot\frac{\gamma-1}{2}\cdots$ Werten

besitzt, und es ist demnach die Gesamtzahl der linearen Formen gleich $2(\alpha - 1)(\beta - 1)(\gamma - 1)\ldots$

Wenn die Zahl c einen quadratischen Faktor enthielte, so könnte man sie durch diesen Faktor dividieren, da die Formel $t^2 + c\vartheta^2 u^2$ nicht allgemeiner ist als $t^2 + cu^2$ und keine anderen zu c primen Teiler besitzt. Man kann demnach immer voraussetzen, dafs c das Produkt von mehreren ungleichen Primzahlen, 2 nicht ausgenommen, ist, so dafs die beiden soeben untersuchten allgemeinen Fälle absolut alle möglichen Fälle einschliefsen. Und obschon wir bisher nur den Fall eines positiven c betrachtet haben, so würde man endlich auch die Formel $t^2 - cu^2$ auf dieselbe Weise behandeln können und würde, was die Anzahl der Formen $4cz + a$ anlangt, welche den Teilern dieser Formel zukommen, dieselben Resultate erhalten. In allen diesen Fällen aber kann man diese verschiedenen linearen Formen auf eine **einfachere** Weise, die zugleich zu neuen Eigenschaften führt, finden.

206.

Wir haben bereits gesehen (No. 140), dafs die verschiedenen Teiler einer solchen Formel wie $t^2 \pm cu^2$ stets auf die Form gebracht werden können:

$$A = py^2 + 2qyz \pm rz^2,$$

in welcher $pr \mp q^2 = c$ ist, und bei welcher man annehmen kann, dafs $2q$ nicht gröfser als p und r ist. Mit Hülfe dieser Bedingungen kann man leicht a priori alle Formen der Teiler bestimmen, welche einer gegebenen Zahl c entsprechen. Die Formen

$$py^2 + 2qyz \pm rz^2,$$

in denen die Unbestimmten in der zweiten Potenz vorkommen, werden wir fernerhin **quadratische Formen** nennen, um sie von den **linearen** Formen $4cx + a$, mit denen wir uns in diesem und im vorigen Paragraphen beschäftigt haben, zu unterscheiden.

Nehmen wir also an, dafs man für eine gegebene Zahl c zunächst alle quadratischen Formen, welche den Teilern der gegebenen Formel $t^2 \pm cu^2$ zukommen, bestimmt habe, so hat man nur noch diese quadratischen Formen in lineare Formen zu entwickeln. Man erhält auf diese Weise alle linearen Formen, welche den Teilern dieser Formel zukommen, und erlangt überdies den Vorteil, dafs

man den Zusammenhang kennen lernt, in welchem die quadratischen und die linearen Formen zu einander stehen.

Es reduciert sich demnach alles darauf zuzusehen, was aus der Formel $py^2 + 2qyz \pm rz^2$ wird, wenn man darin an Stelle von y und z irgendwelche bestimmte Zahlen setzt und die Resultate auf die Form $4cx + a$ bringt, wobei man die Vielfachen von $4c$ weglassen und nur das Resultat beibehalten kann, welches positiv und kleiner als $4c$ ist.

Nun braucht man bei dieser Substitution y und z nicht gröfser als $2c$ zu nehmen; denn setzt man $2c + y$ und $2c + z$ an Stelle von y und z, so geht die Formel $py^2 + 2qyz \pm rz^2$ über in:

$$p(2c+y)^2 + 2q(2c+y)(2c+z) \pm r(2c+z)^2,$$

und diese Gröfse verwandelt sich in:

$$py^2 + 2qyz \pm rz^2 + 4cM,$$

wo $4cM$ ein Vielfaches von $4c$ ist. Demnach geben diese Werte $2c + y$, $2c + z$ dieselbe lineare Form $4cx + a$, welche y und z gegeben hatten.

Ferner mufs man es vermeiden, y und z Werte zu geben, für welche $py^2 + 2qyz \pm rz^2$ gerade wird; denn wir betrachten hier nur die ungeraden und zu c primen Teiler.

Um diese Bedingung um so sicherer zu erfüllen, ist es gut, den quadratischen Teiler $py^2 + 2qyz \pm rz^2$ so vorzubereiten, dafs r gerade ist. Denn da alsdann p ungerade ist, so gebe man y irgendwelche ungeraden Werte und z nach Belieben gerade oder ungerade Werte. Ist r nicht bereits in dem Teiler eine gerade Zahl, so braucht man nur $y \pm z$ an die Stelle von y zu setzen; dann wird das letzte Glied in der transformierten Form gerade sein. In gewissen Fällen werden wir uns auch veranlafst sehen, den quadratischen Teilern die Form $py^2 + qyz + rz^2$, in welcher die drei Koefficienten ungerade sind, zu geben. Alsdann mufs man der Reihe nach $z = 2u$, $y = 2u$, $z + y = 2u$ setzen; dies liefert drei Formeln, welche die verlangte Bedingung erfüllen, jedoch wird man sehen, dafs die Entwicklung einer dieser Formeln genügt.

207.

Wir betrachten also die Formel:

$$A = py^2 + 2qyz \pm 2mz^2,$$

in welcher

$$2mp \mp q^2 = c$$

ist, und in welcher überdies y und p ungerade Zahlen sein müssen. Nimmt man q und c prim zu einander an, so werden auch p und c prim zu einander sein. Setzt man hierauf $y = 1$, so behaupten wir, dafs die Formel

$$p + 2q\psi \pm 2m\psi^2,$$

in welcher nur noch die eine Unbestimmte ψ vorkommt, alle linearen Formen $4cx + a$ enthält, welche in der gegebenen Formel $py^2 + 2qyz \pm 2mz^2$ enthalten sind.

Dazu mufs man beweisen, dafs man, wie beschaffen auch y und z sein mögen, immer eine unbestimmte Zahl ψ der Art finden kann, dafs

$$\frac{p + 2q\psi \pm 2m\psi^2 - py^2 - 2qyz \mp 2mz^2}{4c}$$

eine ganze Zahl ist. Da nämlich p und $4c$ relative Primzahlen sind, so wird die vorstehende Gröfse eine ganze Zahl sein, wenn das Produkt derselben mit p eine solche ist, d. h. wenn man hat:

$$\frac{(p + q\psi)^2 - (py + qz)^2 \pm c(\psi^2 - z^2)}{4c} = e.$$

Ist nun zunächst $\psi = z + 2\lambda$, so hat man nur der Bedingung zu genügen:

$$\frac{(p + qz + 2q\lambda)^2 - (py + qz)^2}{4c} = e,$$

und dies kann man erreichen, indem man eine neue unbestimmte Zahl ϑ der Art annimmt, dafs

$$p + qz + 2q\lambda = py + qz + 2c\vartheta$$

ist. Diese Gleichung ist aber immer auflösbar, da sie auf die Form

$$q\lambda - c\vartheta = p\,\frac{y-1}{2}$$

gebracht werden kann, wobei c und q prim zu einander sind und überdies die rechte Seite eine ganze Zahl ist.

Um daher sämtliche linearen Formen der Formel

$$A = py^2 + 2qyz \pm 2mz^2$$

zu bestimmen, reicht es hin, diejenigen der einfacheren Formel

$$A = p + 2q\psi \pm 2m\psi^2$$

zu suchen, und dies geschieht, indem man ψ der Reihe nach die Werte 0, 1, 2, 3, ... bis $2c - 1$ oder, falls $q = 0$, nur bis $c - 1$ beilegt. Die Werte von A kann man leicht mit Hülfe ihrer Differenzen berechnen, indem man die Vielfachen von $4c$, so oft sie vorkommen, wegläfst. Alsdann verwerfe man von diesen Resultaten



diejenigen, welche mit andern identisch sind, und die, welche mit c einen gemeinschaftlichen Teiler haben.

208.

Sind q und c nicht prim zu einander, so kann man immer die Formel $py^2 + 2qyz \pm 2mz^2$ leicht in eine andre ähnliche umformen, in welcher q prim zu c ist, so dafs man das soeben angegebene Verfahren als absolut allgemein betrachten mufs. Indessen wollen wir noch ein paar Worte über den besonderen Fall, wo die gegebene Formel

$$y^2 \pm cz^2 \quad \text{oder} \quad ay^2 \pm bz^2$$

ist, hinzufügen.

Ist $A = y^2 \pm cz^2$, so mufs man zwei Fälle unterscheiden, je nachdem c gerade oder ungerade ist.

1) Ist c ungerade, so nehme man zunächst y ungerade und z gerade an; dies reduciert den Wert von A, wenn man die Vielfachen von $4c$ beiseite läfst, auf das einzige Glied y^2. Daraus folgt $A = 1, 9, 25, \ldots$ Sodann nehme man y gerade und z ungerade an. Dies giebt $A = 4u^2 \pm c$, und auf diese Weise bilde man die Reihe: $4 \pm c$, $16 \pm c$, $36 \pm c, \ldots$, indem man stets darauf achtet, dafs die Vielfachen von $4c$ weggelassen werden. Die aus diesen Annahmen sich ergebenden Resultate bilden sämtliche lineare Formen von A.

2) Ist c gerade, so mufs y notwendig ungerade sein, während z beliebig ist. Ist z gerade, so hat man einfach $A = y^2 = 1, 9, 25, \ldots$, und ist z ungerade, so wird $A = y^2 \pm c$, so dafs man die Reihe bilden mufs: $1 \pm c$, $9 \pm c$, $25 \pm c, \ldots$. Beide Systeme zusammen geben sämtliche Formen des Teilers A.

Ist die Zahl $c = ab$, so findet man unter den Teilern von $t^2 \pm cu^2$ notwendigerweise $ay^2 \pm bz^2$. Um die linearen Formen dieses Teilers zu erhalten, gebe man y die aufeinanderfolgenden Werte $1, 2, 3, \ldots$ bis $b - 1$, und z die Werte $1, 2, 3, \ldots a - 1$. Es ist nicht nötig weiter zu gehen, weil sich, wenn man $b + y$ oder $b - y$ für y setzt, die beiden Resultate um ein Vielfaches von $4ab$ oder $4c$ unterscheiden und daher als nicht verschieden zu betrachten sind. Ebenso ist es, wenn man $a + z$ oder $a - z$ für z setzt. Man mufs daher jeden der Werte von ay^2 mit jedem der Werte von $\pm bz^2$ kombinieren. Schon die einzige Bedingung, dafs die Summe eine ungerade Zahl sein soll, schliefst eine Menge Kombinationen aus. Sodann mufs man diejenigen Resultate unterdrücken, welche

identisch mit andern sind, oder welche mit c einen gemeinschaftlichen Teiler haben.

Diesen allgemeinen Vorschriften fügen wir nur noch eine Bemerkung hinzu. In dem Falle $c = 4n + 3$ müssen die linearen Teiler der Formel $t^2 + cu^2$ einfach durch $2cx + a$ anstatt durch $4cx + a$ dargestellt werden, weil alsdann eine und dieselbe quadratische Form die Teiler von der Form $4n + 1$ und die von der Form $4n + 3$ enthält. Im Übrigen ist die Rechnung dieselbe, mit dem einzigen Unterschiede, dafs man, anstatt die Vielfachen von $4c$ zu unterdrücken, diejenigen von $2c$ wegzulassen hat, wodurch die Rechnung noch weit kürzer wird.

209.

Beispiel 1.

Es sei die Aufgabe gestellt, alle, sowohl quadratischen wie linearen, Teiler der Formel $t^2 + 41u^2$ zu finden.

Man suche zunächst die quadratischen Teiler mit Hülfe der Formel:

$$pr - q^2 = 41,$$

in welcher man $q < \sqrt{\frac{41}{3}} < 4$ und $2q < p$ und $< r$ annehmen mufs. Die Rechnung ist folgende:

1) Ist $q = 0$, so ist $pr = 41$, also: $p = 1, \quad r = 41$

2) Ist $q = 1$, so ist $pr = 42$, also: $\begin{cases} p = 3, & r = 14 \\ p = 7, & r = 6 \\ p = 21, & r = 2 \end{cases}$

3) Ist $q = 2$, so ist $pr = 45 = 5.9$ also: $p = 5, \quad r = 9$

4) Ist $q = 3$, so ist $pr = 50$. Jedoch kann man 50 nicht in zwei Faktoren zerlegen, welche beide gröfser als 6 oder von denen der kleinere gleich 6 wäre. Mithin ist die Rechnung zu Ende, und es giebt also nur fünf mögliche Formen für die quadratischen Teiler der gegebenen Formel. Von diesen fünf Formen beziehen sich drei auf die Teiler von der Form $4n + 1$, nämlich:

$$y^2 + 41z^2$$
$$21y^2 + 2yz + 2z^2$$
$$5y^2 + 4yz + 9z^2.$$

Die beiden andern beziehen sich auf die Teiler von der Form $4n + 3$ und sind:

$$3y^2 + 2yz + 14z^2$$
$$7y^2 + 2yz + \ \ 6z^2.$$

Wir suchen nun die linearen Formen, welche diesen quadratischen Formen entsprechen.

Wir nehmen von den Teilern von der Form $4n + 1$ die Form:

$$A = 5y^2 + 4yz + 9z^2,$$

und setzen, da der Koefficient des letzten Gliedes ungerade ist, $y - z$ an Stelle von y; sodann ändern wir das Zeichen von z und erhalten:

$$A = 5y^2 + 6yz + 10z^2.$$

Nach dieser Vorbereitung können wir einfach die Formel betrachten:

$$A = 5 + 6\psi + 10\psi^2.$$

Die Resultate, welche diese Formel liefert, wenn darin nach und nach $\psi = 0, 1, 2, 3, \ldots$ gesetzt wird und die Vielfachen von $4c = 164$ weggelassen werden, sind folgende:

Differenzen:	16,	36,	56,	76,	96,	116,	136,	156,
$A =$	5,	21,	57,	113,	189 = 25,	121,	237 = 73,	209 = 45,
Differenzen:	176 = 12,	32,	52,	72,	92			
$A =$	201 = 37,	49,	81,	133,	205 = 41,	133.		

Beim Resultate $41 = c$ angelangt, sieht man, dafs die vorhergehenden 133, 81, . . . in umgekehrter Reihenfolge wiederkehren müssen, so dafs man also wieder zu dem Gliede 5 gelangt. Man mufs aber auch noch wissen, ob nicht etwa über das Glied 5 hinaus neue Glieder auftreten, die nicht in den bereits gefundenen enthalten sind. Zu dem Zwecke mufs man die Reihe rückwärts fortsetzen, wie folgt:

Differenzen:	− 16,	4,	24,	44,	64,	84,	104,	124,	144,	164 = 0.
$A =$	21,	5,	9,	33,	77,	141,	225 = 61,	165 = 1,	125,	269 = 105.

Wegen der Differenz 0 gehen wir nicht mehr weiter, da wir jetzt sicher sind, dafs die vorhergehenden Glieder wiederkehren und kein neues Glied mehr auftritt. Nimmt man also die gefundenen Resultate zusammen und schliefst $41 = c$ aus, so erhält man die folgenden 20, dem gegebenen Teiler $5y^2 + 4yz + 9z^2$ oder $5y^2 + 6yz + 10z^2$ entsprechenden Formen, nämlich:

$$A = 164x + 1,\ 5,\ 9,\ 21,\ 25;\ 33,\ 37,\ 45,\ 49,\ 57;\ 61,\ 73,$$
$$77,\ 81,\ 105;\ 113,\ 121,\ 125,\ 133,\ 141.$$

Nehmen wir jetzt die quadratische Formel

$$A = y^2 + 41z^2,$$

und setzen wir zunächst z als gerade Zahl voraus, so brauchen wir nur den Wert von y^2 zu entwickeln. Daraus ergeben sich dieselben 20 Formen, die wir soeben gefunden haben. Ist sodann y gerade und z ungerade, so hat man den Wert $A = 4u^2 + 41$ zu entwickeln. Auch hieraus folgen stets dieselben Formen. Schliefslich giebt auch die dritte quadratische Form $A = 21y^2 + 2yz + 2z^2$ für die Teiler von der Form $4n + 1$ dieselben Formen, und in der That schliefsen die gefundenen Formen alle diejenigen ein, welche wir a priori für die Teiler der Formel $t^2 + cu^2$ von der Form $4n + 1$ gefunden haben. Die Entwicklung der verschiedenen Formeln kann also keine andern als die 20 schon in Nr. 198 gefundenen Formen liefern. Man sieht aber auch, dafs jede besondere Formel sie alle liefert, und diese Eigenschaft werden wir sogleich allgemein beweisen.

210.

Ist c eine Primzahl von der Form $4n + 1$, so werden die verschiedenen quadratischen Teiler der Formel $t^2 + cu^2$, welche die Form $4n + 1$ haben, sämtlich dieselben linearen Formen $4cz + a$ liefern, wo a $\frac{c-1}{2}$ Werte hat, die positiv und kleiner als $4c$ sind, und diese Werte werden nichts anderes sein, als die auf die Form $4n + 1$ gebrachten Lösungen der Gleichung $\left(\frac{x}{c}\right) = 1$. Ebenso liefern alle quadratischen Teiler derselben Formel, welche von der Form $4n + 3$ sind, dieselben linearen Formen $4cz + a$, wobei a $\frac{c-1}{2}$ Werte besitzt, welches die auf die Form $4n + 3$ gebrachten Lösungen der Gleichung $\left(\frac{x}{c}\right) = -1$ sind.

Ist nämlich $py^2 + 2qyz + 2mz^2 = A$ ein Teiler der Formel $t^2 + cu^2$ von der Form $4n + 1$, und somit p von der Form $4n + 1$, so mufs man beweisen, dafs die linearen Formen, welche aus dieser Formel sich ergeben, mit denen übereinstimmen, die man aus dem ebenfalls zur Form $4n + 1$ gehörenden Teiler $y^2 + cz^2$ erhalten würde. Ändern wir die unbestimmten Zahlen y und z dieser letzteren Formel, um sie nicht mit den andern zu vermengen, in φ und ψ um, so ist die Aufgabe, zu zeigen, dafs man immer, welches auch y und z sein mögen, φ und ψ derart bestimmen kann, dafs die Gröfse

$$\frac{\varphi^2 + c\psi^2 - (py^2 + 2qyz + 2mz^2)}{4c}$$

eine ganze Zahl ist. Da nun p und $4c$ prim zu einander sind, so



wird diese Gröfse eine ganze Zahl sein, wenn das Produkt derselben mit p eine solche ist, oder wenn man hat:

$$\frac{p\varphi^2 - (py + qz)^2 + c(p\psi^2 - z^2)}{4c} = e.$$

Nun ist aber p von der Form $4n + 1$; mithin wird, wofern man $\psi = z$ oder nur $\psi - z$ gerade annimmt, $p\psi^2 - z^2$ durch 4 teilbar sein, so dafs man nur noch der Gleichung

$$\frac{p\varphi^2 - (py + qz)^2}{4c} = e$$

zu genügen hat. Die Zahl p ist aber (No. 198) als Teiler $4n + 1$ der Formel $t^2 + cu^2$ von der Beschaffenheit, dafs $\left(\frac{p}{c}\right) = 1$ ist; folglich ist c Teiler von $x^2 - p$, und somit läfst sich eine Zahl α von der Art finden, dafs $\alpha^2 - p$ durch c teilbar ist. Nimmt man ferner α ungerade, so ist $\frac{\alpha^2 - p}{4c}$ eine ganze Zahl, und es geht daher die zu befriedigende Gleichung über in:

$$\frac{\alpha^2\varphi^2 - (py + qz)^2}{4c} = e.$$

Diese Gleichung ist immer auflösbar, da man, weil α und $2c$ zu einander prim sind, stets zwei unbestimmte Zahlen φ und ϑ von der Beschaffenheit finden kann, dafs

$$\alpha\varphi - (py + qz) = 2c\vartheta$$

ist. Mithin giebt es keine in dem quadratischen Teiler $py^2 + 2qyz + 2mz^2$ enthaltene lineare Form, welche nicht ebenfalls in dem Teiler $y^2 + cz^2$ enthalten wäre. Den umgekehrten Satz würde man durch eine ähnliche Schlufsfolge beweisen können. Nun schliefst aber die Form $y^2 + cz^2$ alle möglichen linearen Formen ein, da sie sich, wenn man z als gerade Zahl annimmt, auf y^2 reduciert und diese sie sämtlich (No. 195) enthält; mithin sind alle diese Formen auch in dem quadratischen Teiler $py^2 + 2qyz + 2mz^2$ enthalten.

Dasselbe kann man von zwei quadratischen Teilern von der Form $4n + 3$, welche durch

$$py^2 + 2qyz + 2mz^2 \quad \text{und} \quad p'y'^2 + 2q'y'z' + 2m'z'^2$$

dargestellt sind, beweisen. Daraus folgt, dafs, im Falle c eine Primzahl von der Form $4n + 1$ ist, alle quadratischen Teiler von der Form $4n + 1$ dieselben linearen Formen geben, und es reicht somit hin, den ersten quadratischen Teiler $y^2 + cz^2$ oder einfach y^2 zu entwickeln. In eben demselben Falle würden alle quadratischen

Teiler von der Form $4n + 3$ ebenfalls dieselben linearen Formen geben, so daſs man nur einen von diesen Teilern zu entwickeln braucht.

211.

Ist jetzt c eine Primzahl von der Form $4n + 3$, so behaupte ich, daſs jeder quadratische Teiler $py^2 + 2qyz + rz^2$ der Formel $t^2 + cu^2$ dieselben linearen Formen enthält, welche der Teiler $y^2 + cz^2$ giebt, wobei diese linearen Formen durch die Formel $2cx + a$ dargestellt werden.

Dazu hat man zu beweisen, daſs man, wie beschaffen auch y und z sein mögen, stets φ und ψ derart bestimmen kann, daſs die Gröſse

$$\frac{\varphi^2 + c\psi^2 - (py^2 + 2qyz + rz^2)}{2c}$$

eine ganze Zahl ist. Da nun p und $2c$ prim zu einander sind, so wird man, wenn man diese Gröſse mit p multipliciert, die Gleichung aufzulösen haben:

$$\frac{p\varphi^2 - (py + qz)^2 + c(p\psi^2 - z^2)}{2c} = e.$$

Nimmt man zunächst $\psi - z$ gerade an, so ist $p\psi^2 - z^2$ stets durch 2 teilbar; es reicht daher aus, die Gleichung

$$\frac{p\varphi^2 - (py + qz)^2}{2c} = e$$

zu befriedigen. Da aber p ein Teiler von $t^2 + cu^2$ ist, so hat man (No. 199) $\left(\frac{p}{c}\right) = 1$; demnach ist c ein Teiler von $t^2 - p$, und somit kann man $\frac{\alpha^2 - p}{2c} = e$ setzen, wodurch die aufzulösende Gleichung übergeht in:

$$\frac{\alpha^2\varphi^2 - (py + qz)^2}{2c} = e.$$

Dieser Gleichung genügt man aber, wenn man die Unbestimmten φ und ϑ sucht, für welche

$$\alpha\varphi - (py + qz) = 2c\vartheta$$

ist. Diese Gleichung ist stets auflösbar, weil α und $2c$ prim zu einander sind. Mithin sind die in dem quadratischen Teiler

$$py^2 + 2qyz + rz^2$$

enthaltenen linearen Formen auch in dem Teiler

$$y^2 + cz^2$$

enthalten und, da die umgekehrte Eigenschaft sich in derselben Weise zeigen läſst, so folgt aus beiden zusammen, daſs irgend ein quadra-

tischer Teiler $py^2 + 2qyz + rz^2$ absolut alle linearen Formen unter sich begreift, welche den Teilern der Formel $t^2 + cu^2$ zukommen. Ist demnach c eine Primzahl von der Form $4n + 3$, so gehören dieselben linearen Formen zur Gesamtheit der quadratischen Teiler und zu jedem von ihnen im besonderen.

Man wird sehen, dafs es sich **nicht ebenso** verhält, wenn c eine **zusammengesetzte** Zahl ist; alsdann sind die linearen Formen in **mehrere Gruppen** geschieden, welche verschiedenen Systemen von quadratischen Teilern entsprechen. Die Existenz dieser Gruppen ist übrigens eine Folge dessen, was wir a priori über die lineare Form der Teiler bewiesen haben.

212.

Beispiel 2.

Man verlangt die linearen Teiler der Formel $t^2 - 39u^2$ nebst den entsprechenden quadratischen Teilern zu wissen.

Dazu suche man zuerst mit Hülfe der Formel $pr + q^2 = 39$, in der man q alle Werte, die kleiner als $\sqrt{\frac{39}{5}}$ oder < 3 sind, geben kann, alle quadratischen Teiler. Diese Teiler sind:

$$\begin{array}{ll} y^2 - 39z^2 & 39y^2 - \ \ z^2 \\ 3y^2 - 13z^2 & 13y^2 - 3z^2 \\ 19y^2 + 2yz - 2z^2 & 2y^2 - 2yz - 19z^2 \\ 5y^2 + 4yz - 7z^2 & 7y^2 - 4yz - \ \ 5z^2. \end{array}$$

Verfolgt man aber die Methode, vermittelst welcher diese Teiler auf die geringstmögliche Anzahl reduciert werden, so findet man, dafs nur die folgenden vier übrig bleiben:

$$\begin{array}{ll} y^2 - 39z^2 & 39y^2 - z^2 \\ 19y^2 + 2yz - 2z^2 & 2y^2 - 2yz - 19z^2. \end{array}$$

Es handelt sich also darum, die linearen Formen zu finden, welche diesen quadratischen Formen entsprechen.

1) Der Teiler $y^2 - 39z^2$ reduciert sich, wenn man z gerade annimmt und die Vielfachen von $4 . 39 = 156$ stets wegläfst, auf das einzige Glied y^2, dessen aufeinanderfolgende Werte sind:

Differenzen:	8,	16,	24,	32,	40,	48,	56,	64,	72,	80,	88,	96,
$y^2 =$	1,	9,	25,	49,	81,	121,	13,	69,	133,	49,	129,	61,

Differenzen:	104,	112,	120,	128,	136,	144,	152,	4,	12
$y^2 =$	1,	105,	61,	25,	153,	133,	121,	117,	121, u. s. w.



Unterdrückt man in dieser Reihe die durch 3 und durch 13 teilbaren Glieder, so bleiben nur sechs verschiedene Glieder übrig, nämlich 1, 25, 49, 61, 121, 133, so daſs der quadratische Teiler $y^2 - 39z^2$ die linearen Formen umfaſst:

$$156x + 1,\ 25,\ 49,\ 61,\ 121,\ 133.$$

Man braucht nur das Vorzeichen der bestimmten Zahlen zu ändern, oder die Ergänzung derselben zu 156 zu nehmen, dann erhält man die linearen Formen, welche dem Teiler $39y^2 - z^2$ entsprechen. Diese Formen sind daher:

$$156x + 23,\ 35,\ 95,\ 107,\ 131,\ 155.$$

2) Gehen wir jetzt zu einer der beiden andern Formen, etwa zu $19y^2 + 2yz - 2z^2$ über, so brauchen wir nur die Formel

$$19 + 2\psi - 2\psi^2$$

zu entwickeln. Daraus ergeben sich folgende Resultate:

Differenzen:	0,	−4,	−8,	−12,	−16 ,	−20,	−24,	−28,	−32,
Reihe:	19,	19,	15,	7,	−5 = 151,	135,	115,	91,	63,

Differenzen:	−36,	−40 ,	−44,	−48,	−52,	−56	−60,	−64,
Reihe:	31,	−5 = 151,	111,	67,	19,	−33 = 123,	67,	7,

Differenzen:	−68 ,	−72,	−76 ,	−80,	
Reihe:	−57 = 99,	31,	−41 = 115,	39,	−41, u. s. w.

Scheidet man die wiederholt vorkommenden und die durch 3 oder 13 teilbaren Glieder aus, so bleiben nur noch sechs Zahlen übrig, woraus folgt, daſs die quadratische Form $19y^2 + 2yz - 2z^2$ die sechs linearen Formen umfaſst:

$$156x + 7,\ 19,\ 31,\ 67,\ 115,\ 151.$$

Die Ergänzung dieser Zahlen zu 156 giebt die linearen Formen, welche der andern quadratischen Form $2y^2 - 2yz - 19z^2$ entsprechen Dieselben sind:

$$156x + 5,\ 41,\ 89,\ 125,\ 137,\ 149.$$

Wir erhalten also bei diesem Beispiel vier Gruppen von linearen Teilern, von denen jede aus sechs Formen besteht und jede einem quadratischen Teiler derselben Formel entspricht. Dies stimmt überein mit der oben gegebenen Theorie, nach welcher sich, wenn die Zahl c das Produkt von zwei Primzahlen α und β ist, das vollständige System der linearen Teiler in 2^2 Gruppen, von denen jede aus $\frac{\alpha - 1}{2} \cdot \frac{\beta - 1}{2}$ Gliedern besteht, zerlegen muſs. In der That ist in

unserm Falle $\alpha = 3$, $\beta = 13$, also $\frac{3-1}{2} \cdot \frac{13-1}{2} = 6$, und jede Gruppe besteht aus sechs Gliedern.

213.

Beispiel 3.

Die Formel $t^2 + 105u^2$ besitzt $5y^2 + 21z^2$ als einen ihrer Teiler. Man wünscht die linearen Formen zu wissen, welche diesem quadratischen Teiler entsprechen.

Nehmen wir zunächst y ungerade und z gerade, so giebt das Glied $5y^2$, wenn man es allein entwickelt und die Vielfachen von $4c$ oder von 420 wegläſst, eine Reihe, welche sich auf die sieben Glieder 5, 45, 125, 185, 245, 285, 405 reduciert. Das andere Glied $21z^2$, in welchem z gerade sein soll, giebt nur die beiden Glieder 84 und 336. Man muſs demnach 84 und 336 zu den sieben vorhergehenden Gliedern addieren. Dies liefert die vierzehn Glieder:

$$89, 129, 209, 269, 329, 369, \ 69$$
$$341, 381, \ 41, 101, 161, 201, 321.$$

Scheidet man hiervon diejenigen aus, welche mit 105 einen gemeinschaftlichen Teiler haben, so bleiben nur die sechs Glieder übrig:

$$41, 89, 101, 209, 269, 341.$$

Man würde genau dieselben sechs Glieder finden, wenn man in dem Teiler $5y^2 + 21z^2$ z ungerade und y gerade annähme. Es giebt daher nur sechs lineare, dem Teiler $5y^2 + 21z^2$ entsprechende Formen, nämlich:

$$420x + 41, 89, 101, 209, 269, 341.$$

214.

Beispiel 4.

Dieselbe Formel $t^2 + 105u^2$ besitzt den quadratischen Teiler $13y^2 + 10yz + 10z^2$. Da aber in diesem Teiler $q = 5$ und 5 ein Teiler von 105 ist, so darf man dem quadratischen Teiler nicht die Form $13 + 10\psi + 10\psi^2$ geben, da das Resultat unvollständig werden würde. Man muſs demnach durch eine Substitution (No. 208) es so einrichten, daſs das mittlere Glied der Formel mit 105 keinen gemeinschaftlichen Faktor mehr hat. Man findet aber bald, daſs, wenn man $y + 2z$ für y setzt, die transformierte Formel

$$13y^2 + 62yz + 82z^2$$

entsteht, welche die verlangte Bedingung erfüllt. Man hat daher jetzt

noch die Formel $13 + 62\psi + 82\psi^2$ zu entwickeln. Die Rechnung ist folgende:

Differenzen: 144, 308, 52, 216, 380, 124, 288, 32, 196, 360

Reihe: 13, 157, 45, 97, 313, 273, 397, 265, 297, 73.

Es ist überflüssig, weiter zu gehen, weil die Rechnung sechs verschiedene Glieder liefert. Demnach sind die linearen Formen, welche dem quadratischen Teiler $13y^2 + 10yz + 10z^2$ entsprechen:

$$420x + 13,\ 73,\ 97,\ 157,\ 313,\ 397.$$

Im Übrigen ist das vollständige System der quadratischen Teiler von $t^2 + 105u^2$ nebst den entsprechenden linearen Formen:

Quadratische Teiler:	Entsprechende lineare Teiler:
$y^2 + 105z^2$	$420x +$ 1, 109, 121, 169, 289, 361
$53y^2 + 2yz + 2z^2$	$420x +$ 53, 113, 137, 197, 233, 317
$5y^2 + 21z^2$	$420x +$ 41, 89, 101, 209, 269, 341
$13y^2 + 10yz + 10z^2$	$420x +$ 13, 73, 97, 157, 313, 397
$3y^2 + 35z^2$	$420x +$ 47, 83, 143, 167, 227, 383
$19y^2 + 6yz + 6z^2$	$420x +$ 19, 31, 139, 199, 271, 391
$7y^2 + 15z^2$	$420x +$ 43, 67, 127, 163, 247, 403
$11y^2 + 14yz + 14z^2$	$420x +$ 11, 71, 179, 191, 239, 359.

Es giebt daher im Ganzen acht Gruppen von linearen Teilern, von denen jede aus sechs Gliedern besteht. Und in der That mufs man, da 105 das Produkt der drei Faktoren 3, 5, 7 ist, der oben gegebenen Theorie zufolge 2^3 Gruppen erhalten, deren jede aus $\frac{3-1}{2} \cdot \frac{5-1}{2} \cdot \frac{7-1}{2} = 6$ Gliedern besteht. Wir sehen ferner bei dieser Entwicklung, dafs jede Gruppe einem und nur einem quadratischen Teiler entspricht.

§ 11.

Erklärung der Tafeln III, IV, V, VI und VII.

215.

Tafel III.

Die Tafel III enthält alle quadratischen Teiler der Formel $t^2 - cu^2$, sowie die entsprechenden linearen Teiler. Sie ist berechnet für alle Zahlen von $c = 2$ bis $c = 79$ mit Aus-

nahme derer, welche Quadratzahlen oder durch eine Quadratzahl teilbar sind. Die letzteren sind ausgeschlossen, weil die Teiler der Formel $t^2 - c\vartheta^2 u^2$, wenn sie prim zu $c\vartheta^2$ genommen werden, dieselben sind, wie diejenigen der Formel $t^2 - cu^2$.

Die quadratischen Teiler, welche allgemein durch die Formel $py^2 + 2qyz - rz^2$, wo $pr + q^2 = c$ ist, dargestellt werden, sind nach der Methode des § 13 Hauptteil I auf die geringstmögliche Anzahl reduciert.

Neben jedem quadratischen Teiler $py^2 + 2qyz - rz^2$ mufs der zu ihm inverse $ry^2 + 2qyz - pz^2$ vorkommen. Indessen sind diese beiden Formen zuweilen mit einander identisch, und zwar tritt dies ein, wenn man der Gleichung $m^2 - cn^2 = -1$ genügen kann (No. 93). In diesem Falle ist in die Tafel nur die eine der beiden Formen, welche identisch sein sollen, aufgenommen.

Neben jedem quadratischen Teiler stehen die aus ihm sich ergebenden, nach der Methode des vorhergehenden Paragraphen berechneten linearen Teiler. Diese Teiler sind prim zu c vorausgesetzt und ferner sind nur die ungeraden Teiler in Betracht gezogen, obwohl die Formeln $py^2 + 2qyz - rz^2$ auch gerade Zahlen einschliefsen.

Bei dieser Tafel bemerkt man durchgehends, dafs sich die linearen Teiler in mehrere Gruppen zerlegen, deren Anzahl ebenso wie die Menge der in einer jeden von ihnen enthaltenen Glieder mit dem allgemeinen Gesetze (No. 205) im Einklang steht. Indessen kommt es bisweilen vor, dafs zwei von diesen Gruppen zusammengefafst sind und daher einer und derselben quadratischen Form entsprechen. Ist z. B. $c = 66 = 2 \cdot 3 \cdot 11$, so sagt der allgemeine Satz, dafs es 2^3 oder 8 Gruppen mit je $\frac{3-1}{2} \cdot \frac{11-1}{2} = 5$ Gliedern gebe. In der Tafel findet man aber nur vier Gruppen mit je 10 Gliedern, und zwar deshalb, weil zwei Gruppen zu einer einzigen zusammengefafst sind. Übrigens ist die Gesamtzahl der linearen Formen in beiden Fällen 40, wie es der Theorie zufolge sein mufs.

216.

Tafel IV.

Die Tafel IV enthält sowohl die quadratischen wie die linearen Teiler der Formel $t^2 + au^2$ für jede Zahl a von der Form $4n + 1$, welche nicht Quadratzahl oder durch eine Quadratzahl teilbar ist, und zwar für alle Zahlen von 1 bis 105.

Die erste Formel $t^2 + u^2$, welche nur einen einzigen quadra-

tischen Teiler $y^2 + z^2$ besitzt, hat auch nur den einzigen linearen Teiler $4x + 1$. Alle andern Formeln $t^2 + 5u^2$, $t^2 + 13u^2$, u. s. w. besitzen gleichzeitig Teiler von der Form $4n + 1$ und solche von der Form $4n + 3$. Es ist ferner zu bemerken, 1) dafs die quadratischen Teiler, welche die Zahlen von der Form $4n + 1$ enthalten, immer verschieden sind von denen, welche die Zahlen von der Form $4n + 3$ enthalten; 2) dafs es stets ebensoviele lineare Formen für die Teiler von der Form $4n + 1$ giebt, als es deren für die Teiler von der Form $4n + 3$ giebt. Dasselbe ist nicht immer der Fall bei den quadratischen Teilern. Z. B. sieht man, dafs die Formel $t^2 + 41u^2$ drei quadratische Teiler von der Form $4n + 1$ und nur zwei von der Form $4n + 3$ besitzt. Ebenso besitzt die Formel $t^2 + 65u^2$ vier Teiler der ersten und nur zwei der zweiten Art.

217.

In dieser Tafel ist mit der allgemeinen Form der quadratischen Teiler $py^2 + 2qyz + rz^2$ eine leichte Änderung vorgenommen; sie besteht darin, dafs q beständig ungerade vorausgesetzt ist. Da alsdann $q^2 + a$ oder pr eine gerade Zahl ist, so kann man $2m$ für r setzen, wodurch die Form der quadratischen Teiler übergeht in

$$py^2 + 2qyz + 2mz^2,$$

wobei die Zahlen p und m stets ungerade sind.

Diese Form bietet den Vorteil, dafs sie unmittelbar eine andere

$$2py^2 + 2qyz + mz^2$$

liefert. Diese beiden Formen werden wir wegen des Zusammenhanges, in welchem sie mit einander stehen, von nun an **konjugierte Formen** oder **konjugierte Teiler** nennen.

Wir haben behauptet, dafs die Zahlen p und m stets ungerade sind; da nämlich q^2 von der Form $8n + 1$ und a von der Form $4n + 1$ ist, so ist offenbar $q^2 + a$ oder $2pm$ von der Form $4n + 2$; mithin ist pm notwendig ungerade. Jedoch mufs man zwei Fälle unterscheiden, je nachdem a von der Form $8n + 1$ oder $8n + 5$ ist.

1) Ist a von der Form $8n + 1$, so ist $q^2 + a$ von der Form $8n + 2$ und pm von der Form $4n + 1$. Dies kann aber nur stattfinden, sobald die Zahlen p und m alle beide von der Form $4n + 1$ oder alle beide von der Form $4n + 3$ sind. Alsdann gehören somit die konjugierten Formen

$$py^2 + 2qyz + 2mz^2 \text{ und } 2py^2 + 2qyz + mz^2$$

alle beide zu den Teilern von der Form $4n + 1$ oder alle beide zu den Teilern von der Form $4n + 3$.



2) Ist a von der Form $8n+5$, so ist pm von der Form $4n+3$, so daſs von den beiden Zahlen p und m die eine von der Form $4n+1$, die andere von der Form $4n+3$ ist. Alsdann gehört somit von den beiden konjugierten Formen die eine zu den Teilern von der Form $4n+1$, die andere zu den Teilern von der Form $4n+3$. Demnach sieht man, daſs, wenn a irgend eine Zahl von der Form $8n+5$ ist, die Formel t^2+au^2 stets ebenso viele quadratische Teiler von der Form $4n+1$ wie quadratische Teiler von der Form $4n+3$ besitzt.

218.

Sind die quadratischen Teiler der Formel t^2+au^2 nach der allgemeinen Methode gefunden, so ist es immer leicht, sie auf die Form $py^2+2qyz+2mz^2$ zu bringen, in welcher q ungerade ist; denn man hat nur diejenigen, in denen q gerade ist, zu transformieren, indem man nur $y-z$ für z setzt.

Man kann aber auch direkt alle quadratischen Teiler einer gegebenen Formel t^2+au^2 in der Form $py^2+2qyz+2mz^2$ finden. Dazu beachte man, daſs, wenn man q ungerade sein läſst, man immer bewirken kann, daſs q weder p noch m übersteigt. Denn setzt man, falls $q>p$ ist, $y-2\alpha z$ an die Stelle von y, oder, falls $q>m$ ist, $z-\alpha y$ an die Stelle von z, so kann man leicht die Zahl α derart bestimmen, daſs in der transformierten Formel $q<p$ oder $q<m$ ist. Mithin kann vermittelst einer oder mehrerer solcher Substitutionen jede Formel $py^2+2qyz+2mz^2$, in welcher $2pm-q^2=a$ ist, auf eine ähnliche Formel zurückgeführt werden, in welcher q weder p noch m übersteigt, so daſs $2pm-q^2>q^2$ und somit $q<\sqrt{a}$ ist.

Um daher alle quadratischen Formen $py^2+2qyz+2mz^2$, welche den Teilern der Formel t^2+au^2 zukommen, zu erhalten, muſs man q der Reihe nach die ungeraden Werte $1, 3, 5, \ldots$ bis $\sqrt{a}$ geben. Jeder Wert von q liefert einen für $pm=\frac{q^2+a}{2}$. Läſst sich dieser Wert in zwei Faktoren p und m, die nicht kleiner als q sind, zerlegen, so ergeben sich daraus die beiden konjugierten Teiler:

$$py^2+2qyz+2mz^2 \quad \text{und} \quad 2py^2+2qyz+mz^2.$$

Diese Methode liefert ebenso wie die allgemeine Methode alle möglichen Formen der quadratischen Teiler; sie führt jedoch weit schneller zum Ziele, da man nur die Werte von q, welche ungerade und kleiner als $\sqrt{a}$ sind, zu versuchen hat, während man bei der allgemeinen Methode den Versuch mit allen, geraden wie ungeraden,

Werten von q bis zu $\sqrt{\frac{1}{3}a}$ anstellen mufs. Es ist aber:

$$\frac{1}{2}\sqrt{a} < \sqrt{\frac{1}{3}a}.$$

Dieser neuen Methode entsprechend wird der quadratische Teiler $y^2 + az^2$ dargestellt durch die Formel

$$y^2 + 2yz + (a+1)z^2,$$

und der zu ihm konjugierte ist:

$$2y^2 + 2yz + \left(\frac{a+1}{2}\right)z^2.$$

Der gröfseren Gleichmäfsigkeit wegen ist in der Tafel die Form $y^2 + 2yz + (a+1)z^2$ belassen worden mit Ausnahme des ersten Feldes, wo man die Einfachheit des Teilers $y^2 + z^2$ nicht dadurch stören wollte, dafs man $y^2 + 2yz + 2z^2$ an seine Stelle setzt.

In allen Fällen sind die linearen Formen aus den quadratischen Formen mittelst der Methoden des vorigen Paragraphen abgeleitet worden. Die Anzahl der Gruppen und ebenso die Anzahl der in jeder von ihnen enthaltenen Glieder ist stets in Übereinstimmung mit dem allgemeinen Gesetze.

219.

Tafel V.

Die Tafel V enthält sowohl die quadratischen wie die linearen Teiler der Formel $t^2 + au^2$, wo a eine Zahl von der Form $4n + 3$ ist, die weder Quadratzahl noch durch eine Quadratzahl teilbar ist.

Die quadratischen Teiler haben ihre gewöhnliche Form behalten, sobald $a = 8n + 7$ ist, sie sind jedoch etwas abgeändert worden in dem Falle, wo $a = 8n + 3$ ist. Dies wollen wir jetzt erläutern.

Ist a von der Form $8n + 3$, und bezeichnet man mit P einen beliebigen ungeraden Teiler der Formel $t^2 + au^2$, so kann man immer t und u als ungerade voraussetzen. Da alsdann $t^2 + au^2$ von der Form $8n + 4$ ist, so wird der Quotient, welchen man erhält, wenn man $t^2 + au^2$ durch P dividiert, notwendig von derselben Form $8n + 4$ oder $4p$ sein, wo p eine ungerade Zahl ist. Man hat daher:

$$t^2 + au^2 = 4Pp.$$

In dieser Gleichung sind die Zahlen u und $2p$ prim zu einander; denn hätten sie einen gemeinschaftlichen Teiler, so würden auch t und u einen solchen haben, was gegen die Voraussetzung ist. Mithin kann man $u = z$ und $t = 2py + qz$ setzen, wodurch man erhält:

$$P = py^2 + qyz + \frac{q^2 + a}{4p}z^2.$$

Diese Gleichung kann aber nur dann bestehen, wenn $\frac{q^2 + a}{4p}$ eine ganze Zahl ist. Setzt man also $q^2 + a = 4pr$, so ergiebt sich:

$$P = py^2 + qyz + rz^2.$$

In dieser Formel sind die drei Koefficienten p, q, r ungerade; denn zunächst ist, da t ungerade und $t = 2py + qz$ ist, offenbar auch q ungerade. Da ferner q^2 von der Form $8n + 1$ und a von der Form $8n + 3$ ist, so ist $q^2 + a$ von der Form $8n + 4$, und somit $\frac{q^2 + a}{4}$ oder pr ungerade. Folglich sind p und r selbst ungerade.

Man erkennt hieraus, dafs jeder ungerade Teiler der Formel $t^2 + au^2$ stets auf die Form $py^2 + qyz + rz^2$, in welcher p, q, r ungerade Zahlen und $4pr - q^2 = a$ ist, gebracht werden kann. Ich behaupte ferner, dafs man in dieser Formel den mittleren Koefficienten q kleiner oder wenigstens nicht gröfser als jeden der äufseren p, r voraussetzen darf. Denn wäre z. B. $q > p$, so setze man $y - \alpha z$ an die Stelle von y; da hierdurch der mittlere Koefficient in $q - 2\alpha p$ übergeht, so kann man mit Hülfe der unbestimmten Zahl α diesen Koefficienten kleiner oder wenigstens nicht gröfser als p machen.

Da somit p und r gröfser oder wenigstens nicht kleiner als q sind, so ist offenbar:

$$4pr - q^2 > 3q^2,$$

und daher:

$$q < \sqrt{\frac{a}{3}}.$$

Will man also alle quadratischen Formen wissen, welche den ungeraden Teilern der Formel $t^2 + au^2$ zukommen, so hat man q der Reihe nach die ungeraden Werte 1, 3, 5 bis $\sqrt{\frac{a}{3}}$ beizulegen. Jeder Wert von q giebt einen Wert für $pr = \frac{q^2 + a}{4}$; läfst sich dieser Wert in zwei Faktoren zerlegen, die nicht kleiner sind als q, so entsteht aus diesen eine der gesuchten quadratischen Formen.

220.

Ist z. B. $a = 91$ und setzt man $q = 1$, so wird:

$$\frac{q^2 + a}{4} = 23 = 1 \cdot 23.$$

Hieraus entsteht der Teiler $y^2 + yz + 23z^2$.

Setzt man $q = 3$, so wird:

$$\frac{q^2 + a}{4} = 25 = 5 \cdot 5.$$

Hieraus entsteht ein zweiter Teiler $5y^2 + 3yz + 5z^2$.

Da $\sqrt{\frac{91}{3}}$ die Grenze von q ist, so könnte man noch $q = 5$ setzen, wodurch sich $\frac{q^2 + a}{4} = 29$ ergeben würde. Da aber diese Zahl eine Primzahl ist, so entsteht daraus kein neuer Teiler. Demnach sind die beiden gefundenen Formeln die einzigen quadratischen Teiler von $t^2 + 91u^2$.

Ist noch $a = 163$, so kann man, da $\sqrt{\frac{163}{3}} < 9$ die Grenze von q ist, der Reihe nach $q = 1, 3, 5, 7$ setzen, wodurch sich $pr = 41, 43, 47, 53$ ergiebt. Da aber diese Zahlen Primzahlen sind, so folgt daraus, dafs die Formel $t^2 + 163u^2$ nur den einen quadratischen Teiler $y^2 + yz + 41z^2$ haben kann.

221.

Die Formel $py^2 + qyz + rz^2$, deren Koefficienten ungerade sind, stellt im Allgemeinen drei quadratische Teiler von der gewöhnlichen Form, in welcher der mittlere Koefficient gerade ist, dar. Denn bei Anwendung dieser Formel mufs man die Zahlen y und z entweder alle beide ungerade oder die eine gerade, die andere ungerade annehmen. Man kann somit nur die drei Annahmen

$$z = 2u, \quad y = 2u, \quad y = 2u - z$$

machen, und diese geben die drei Formen:

$$py^2 + 2qyu + 4ru^2$$
$$4pu^2 + 2qzu + rz^2$$
$$4pu^2 + (2q - 4p)uz + (p - q + r)z^2.$$

Diese drei Formen reducieren sich auf zwei, wenn zwei der Zahlen p, q, r gleich sind. Sie reducieren sich auf eine einzige, wenn die Zahlen p, q, r unter einander gleich sind. Dieser Fall kann aber nur eintreten, wenn sie gleich der Einheit sind, oder wenn $t^2 + 3u^2$ die gegebene Formel ist, denn alsdann reduciert sich der Teiler $y^2 + yz + z^2$, wie wir bereits (No. 143) gefunden haben, auf die eine Form $y^2 + 3z^2$. In jedem andern Falle sind die soeben entwickelten Formeln, oder wenigstens zwei von ihnen, wesentlich von einander verschieden. Es folgt daraus, dafs sich die Anzahl der quadratischen Teiler bedeutend vermindert, wenn man dieselben durch die ungerade Koefficienten besitzende Formel $py^2 + qyz + rz^2$ darstellt. Übrigens kann man, wie wir soeben gesehen haben, aus diesen



Teilern mit ungeraden Koefficienten leicht die quadratischen Teiler von der gewöhnlichen Form ableiten, wodurch man eine beinahe dreifache Anzahl erhält.

222.

Es ist nützlich zu bemerken, dafs die in der Tafel V enthaltenen quadratischen Teiler sowohl für den Fall $a = 8n + 3$ als für den Fall $a = 8n + 7$ stets auf die Form

$$py^2 + 4\varphi yz + \pi z^2$$

gebracht werden können, welche sich von der allgemeinen Form

$$py^2 + 2qyz + rz^2$$

nur dadurch unterscheidet, dafs in ihr q gerade ist. Hat man nämlich nach der allgemeinen Methode alle quadratischen Teiler

$$py^2 + 2qyz + rz^2$$

der Formel $t^2 + au^2$ gefunden, so sind nur noch diejenigen, in welchen q ungerade ist, zu transformieren. Da nun alsdann die eine der Zahlen p und r gerade, die andere ungerade sein mufs, so braucht man nur, wenn p die ungerade Zahl ist, $y - z$ für y zu setzen. Dadurch geht der mittlere Koefficient $2q$ in $2q - 2p$ über; er wird daher von der verlangten Form 4φ.

Weil nun jetzt alle quadratischen Teiler auf die Form

$$py^2 + 4\varphi yz + \pi z^2$$

gebracht sind, und da ferner $p\pi = 4\varphi^2 + a$ ist, so folgt daraus, dafs $p\pi$ von der Form $4n + 3$ und somit von den beiden Koefficienten p und π der eine von der Form $4n + 1$, der andere von der Form $4n + 3$ ist. Man erkennt hieraus, dafs jede quadratische Form

$$py^2 + 4\varphi yz + \pi z^2$$

zu gleicher Zeit sowohl Teiler von der Form $4n + 1$ als auch solche von der Form $4n + 3$ enthält. Es ist jedoch leicht, diese beiden Formen von einander zu trennen, wie es in den Tafeln III und IV der Fall ist. Denn ist p von der Form $4n + 1$, und setzt man $z = 2u$, so stellt die Formel $py^2 + 8\varphi yu + 4\pi u^2$ offenbar nur Teiler von der Form $4n + 1$ dar; setzt man dagegen $y = 2u$, so stellt die Formel $4pu^2 + 8\varphi zu + \pi z^2$ nur Teiler von der Form $4n + 3$ dar.

223.

Was die linearen Formen angeht, welche den quadratischen Teilern entsprechen, so lassen sich dieselben ebenso in zwei Arten, die



einen von der Form $4n + 1$, die andern von der Form $4n + 3$ teilen. Es genügt, dies an einem Beispiel zu entwickeln.

Aus der Tafel sieht man, dafs die Formel

$$t^2 + 11u^2$$

nur den einen quadratischen Teiler mit ungeraden Koefficienten

$$y^2 + yz + 3z^2$$

besitzt. Dieser Teiler schliefst zwei andere von gewöhnlicher Form ein, nämlich:

$$y^2 + 11z^2$$
$$3y^2 + 2yz + 4z^2.$$

Von diesen beiden Teilern, welche man nach der allgemeinen Methode unmittelbar gefunden haben würde, besitzt der eine den mittleren Koefficienten 0, welcher zur Form 4φ gehört. Um den andern auf dieselbe Form zu bringen, mufs man $y - z$ an die Stelle von z setzen, wodurch man die transformierte Formel

$$3y^2 + 4yz + 5z^2$$

erhält. Somit ergeben sich zwei quadratische Teiler von der Form $4n + 1$, nämlich:

$$y^2 + 44z^2$$
$$5y^2 + 8yz + 12z^2,$$

und zwei quadratische Teiler von der Form $4n + 3$, nämlich:

$$11y^2 + 4z^2$$
$$3y^2 + 8yz + 20z^2.$$

Was die entsprechenden linearen Formen angeht, so leitet man dieselben leicht aus den in den Tafeln gegebenen, nämlich aus

$$22x + 1,\ 3,\ 5,\ 9,\ 15$$

ab. Um daher diejenigen von der Form $4n + 1$ zu erhalten, behalte man die bestimmten Zahlen 1, 5, 9, welche von dieser Form sind, bei und addiere 22 zu den beiden andern 3 und 15. Dies giebt im Ganzen die fünf Formen:

$$44x + 1,\ 5,\ 9,\ 25,\ 37.$$

In ähnlicher Weise findet man die Formen $4n + 3$, nämlich:

$$44x + 3,\ 15,\ 23,\ 27,\ 31.$$

Will man daher in der Tafel die Formen $4n + 1$ von den Formen $4n + 3$ trennen, so mufs man an Stelle der in der Tafel befindlichen, auf die Teiler von $t^2 + 11u^2$ bezüglichen Spalte die folgende setzen:

Quadratische Teiler:	Lineare Teiler:
$y^2 + 44z^2$ $5y^2 + 8yz + 12z^2$	$44x + 1, 5, 9, 25, 37$
$11y^2 + 4z^2$ $3y^2 + 8yz + 20z^2$	$44x + 3, 15, 23, 27, 31.$

Es ist nicht nötig, darauf hinzuweisen, dafs die in der Tafel befindliche Spalte zwar viel kürzer, aber darum nicht weniger allgemein ist.

224.

Um nichts unerwähnt zu lassen, wodurch man die Aufsuchung der quadratischen Teiler abkürzen kann, wollen wir schliefslich noch ein paar Worte über den Fall $a = 8n + 7$ hinzufügen. Ist also $a = 8n + 7$, und nimmt man q in dem quadratischen Teiler

$$py^2 + 2qyz + rz^2$$

als ungerade an, so wird dieser Teiler die Form

$$py^2 + 2qyz + 8mz^2$$

annehmen, wobei $pm = \frac{q^2 + a}{8}$. In dieser Form kann man q kleiner als $4m$ und nicht gröfser als p voraussetzen; mithin wird $q < \sqrt{a}$ sein. Man setze also versuchsweise für q alle ungeraden Zahlen 1, 3, 5, ... bis $\sqrt{a}$, berechne für jeden Wert von q den Wert von $pm = \frac{q^2 + a}{8}$ und sehe zu, ob sich dieser Wert in zwei Faktoren zerlegen läfst, von denen der eine p ungerade und nicht kleiner als q, der andere m gerade oder ungerade, aber gröfser als $\frac{q}{4}$ ist. So vielmal diese Bedingung sich erfüllen läfst, so viele quadratische Teiler der Formel $t^2 + au^2$ erhält man. Diese Teiler können sodann entweder auf die gewöhnliche Form, in welcher $2q < p$ und $< r$ ist, oder auf die früher erwähnte Form, in welcher q gerade ist, gebracht werden. Dieses Verfahren führt sehr schnell zum Ziele, da man immer nur mit Zahlen pm, die kleiner als $\frac{a}{4}$ sind, zu rechnen hat, während bei der allgemeinen Methode pr bis zu $\frac{4a}{3}$ gehen kann.

225.

Tafel VI.

Die Tafel VI enthält sowohl die quadratischen wie die linearen Teiler der Formel $t^2 + 2au^2$, wo a eine Zahl von der Form $4n + 1$ ist, die weder selbst eine Quadratzahl noch durch eine Quadratzahl teilbar ist.

Die quadratischen Teiler sind auf die Form

$$py^2 + 4\varphi yz + 2mz^2,$$

in welcher

$$pm = 2\varphi^2 + a$$

ist, gebracht. Es ist aber leicht zu sehen, dafs man, ohne diese Form zu ändern, 2φ kleiner oder nicht gröfser als p und m voraussetzen darf, so dafs $pm > 4\varphi^2$ und $\varphi < \sqrt{\frac{1}{2}a}$ ist. Genügt man also mit Rücksicht auf diese Bedingungen der Gleichung $pm = 2\varphi^2 + a$ auf alle möglichen Weisen, so erhält man dadurch unmittelbar für die Formel $t^2 + 2au^2$ sämtliche quadratischen Teiler in der Form $py^2 + 4\varphi yz + 2mz^2$. Dieses Verfahren ist viel kürzer als die allgemeine Methode, da $\sqrt{\frac{1}{2}a}$ kleiner ist als $\sqrt{\frac{8}{3}a}$.

Jede Form $py^2 + 4\varphi yz + 2mz^2$ ergiebt sich mit der zu ihr konjugierten Form $2py^2 + 4\varphi yz + mz^2$ gleichzeitig aus demselben, den verlangten Bedingungen genügenden Werte von pm.

Ist die Zahl p von der Form $8n+1$ oder $8n+3$, so enthält der quadratische Teiler $py^2 + 4\varphi yz + 2mz^2$ nur Zahlen derselben Formen $8n+1$ oder $8n+3$. Denn da y stets ungerade ist, so wird der in Rede stehende Teiler, falls z gerade ist, von der Form $p + 8k$, also von derselben Form wie p sein. Ist aber z ungerade, so wird der quadratische Teiler, wenn man die Vielfachen von 8 wegläfst, von der Form $p + 4\varphi + 2m$. Es sei nun zunächst $p = 8n + 1$; dann erhält man (immer mit Weglassung der Vielfachen von 8) wegen $pm = 2\varphi^2 + a$:

$$m = 2\varphi^2 + a,$$

und somit:

$$p + 4\varphi + 2m = 1 + 4\varphi + 4\varphi^2 + 2a = 1 + 2a = 3.$$

Mithin wird der quadratische Teiler von der Form $8n + 3$. Zweitens sei $p = 8n + 3$, so erhält man:

$$3m = 2\varphi^2 + a$$
$$6m = 4\varphi^2 + 2a$$

und

$$p + 4\varphi + 2m = 3 + 4\varphi - 4\varphi^2 - 2a = 3 - 2a = 1.$$

Mithin ist der Teiler von der Form $8n + 1$.

Ebenso beweist man, dafs, wenn p eine der Formen $8n+5$, $8n+7$ besitzt, der quadratische Teiler $py^2 + 4\varphi yz + 2mz^2$ nur Zahlen von denselben Formen $8n+5$, $8n+7$ enthalten kann.

Mithin zerfallen alle quadratischen Teiler der Formel $t^2 + 2au^2$, in welcher a von der Form $4n+1$ ist, in zwei Arten, von denen

die eine alle Teiler von der Form $8n+1$ und $8n+3$, die andere alle Teiler von der Form $8n+5$ und $8n+7$ enthält.

226.

Jeder in der Tafel befindliche quadratische Teiler enthält beide Formen gleichzeitig; indessen lassen sich dieselben dem vorangegangenen Beweise zufolge leicht von einander trennen.

Ist die Formel t^2+42u^2 gegeben, und betrachten wir zunächst den quadratischen Teiler

$$y^2+42z^2,$$

welchem die linearen Formen

$$168x+1,\ 25,\ 43,\ 67,\ 121,\ 163$$

entsprechen, so gehört dieser quadratische Teiler augenscheinlich zu den Formen $8n+1$, $8n+3$. Um diese von einander zu trennen, bemerke ich, dafs, wenn z gerade ist, oder wenn man $2z$ an die Stelle von z setzt, der Teiler in y^2+168z^2 übergeht und nur noch die Formen $8n+1$ enthält. Setzt man dagegen gleichzeitig y und z ungerade voraus, oder setzt man, um diese Bedingung zu beseitigen, $2y+z$ an die Stelle von y, so geht der Teiler in $4y^2+4yz+43z^2$ über und enthält nur noch die Formen $8n+3$. Behandelt man in gleicher Weise die drei andern quadratischen Teiler der gegebenen Formel t^2+42u^2, so erhält man die folgenden Resultate:

Quadratische	Lineare
Teiler $8n+1$	
y^2+168z^2	$168x+1,\ 25,\ 121$
$17y^2+12yz+12z^2$	$168x+17,\ 41,\ 89$
Teiler $8n+3$	
$43y^2+4yz+4z^2$	$168x+43,\ 67,\ 163$
$3y^2+56z^2$	$168x+59,\ 83,\ 131$
Teiler $8n+5$	
$21y^2+8z^2$	$168x+29,\ 53,\ 149$
$13y^2+24yz+24z^2$	$168x+13,\ 61,\ 157$
Teiler $8n+7$	
$7y^2+24z^2$	$168x+31,\ 55,\ 103$
$23y^2+8yz+8z^2$	$168x+23,\ 71,\ 95$

Wie man sieht, zerfallen die linearen Teiler in acht Gruppen von je drei Gliedern, was mit dem allgemeinen Gesetze (No. 205) übereinstimmt.

227.

Tafel VII.

Die Tafel VII enthält die linearen und quadratischen Teiler der Formel $t^2 + 2au^2$, in welcher a eine Zahl von der Form $4n + 3$ ist, die sich nicht durch eine Quadratzahl teilen läfst.

Die quadratischen Teiler sind, wie in der vorhergehenden Tafel, auf die Form

$$py^2 + 4\varphi yz + 2mz^2$$

gebracht, in welcher

$$mp = 2\varphi^2 + a$$

ist, so dafs die Bestimmung dieser Formen immer in derselben Weise geschieht.

Ist der Koefficient p von der Form $8n + 3$ oder $8n + 5$, so enthält der quadratische Teiler $py^2 + 4\varphi yz + 2mz^2$ nur Zahlen von der Form $8n + 3$ oder $8n + 5$; und ist der Koefficient p von der Form $8n + 1$ oder $8n + 7$, so enthält der Teiler nur Zahlen von eben diesen Formen $8n + 1$ oder $8n + 7$. Dies wird ebenso bewiesen, wie bei der Erklärung der vorigen Tafel.

Es ergiebt sich demnach, dafs alle quadratischen Teiler der Formel $t^2 + 2au^2$, in welcher a eine Zahl von der Form $4n + 3$ ist, in zwei Arten zerfallen, von denen die eine alle Zahlen von der Form $8n + 3$ oder $8n + 5$, die andere alle Zahlen von der Form $8n + 1$ oder $8n + 7$ enthält. Abgesehen aber von diesen ungeraden Zahlen enthält offenbar jeder quadratische Teiler $py^2 + 4\varphi yz + 2mz^2$ auch gerade Zahlen, da man y gerade und z ungerade nehmen kann, wofern sie nur prim zu einander sind.

Ebenso kann man sowohl die quadratischen wie die linearen Teiler in die vier Arten, welche den vier Formen $8n + 1$, $8n + 3$, $8n + 5$, $8n + 7$ entsprechen, zerlegen.

Allgemeine Bemerkung.

Bei diesen verschiedenen Tafeln ist zu bemerken, dafs jede Gruppe von linearen Teilern stets einer und derselben Anzahl von quadratischen Teilern entspricht, wenn man nämlich jeden quadratischen Teiler, welcher von einer der Formen $py^2 + rz^2$, $py^2 + 2qyz + 2qz^2$, $py^2 + 2qyz + pz^2$ ist, nur für $\frac{1}{2}$ rechnet. Der Grund dieser Ausnahme beruht darin, dafs diese Arten von Teilern bei den beiden verschie-

denen Annahmen über die Werte der Unbestimmten y und z die gleiche Anzahl liefern, so daſs sie in Wirklichkeit nur die Hälfte der Anzahl der Teiler, welche in den andern Formen enthalten sind, in sich schlieſsen.

§ 12.

Eine Reihe von Sätzen, welche sich aus den vorher erwähnten Tafeln ergeben.

228.

Allgemeiner Satz. Ist $4cx + a$ eine der linearen Formen, welche den Teilern von $t^2 \pm cu^2$ zukommen, so behaupte ich, daſs jede in der Form $4cx + a$ enthaltene Primzahl notwendig ein Teiler der Formel $t^2 \pm cu^2$ und somit von einer der zur linearen Form $4cx + a$ gehörigen quadratischen Formen $py^2 + 2qyz \pm rz^2$ ist.

Nimmt man z. B. in der Tafel VII die Formel $t^2 + 30u^2$, und wählt man in diesem Beispiel die dem quadratischen Teiler $15y^2 + 2z^2$ entsprechenden linearen Formen, so kann man behaupten, daſs jede Primzahl, welche eine von den Formen

$$120x + 17,\ 23,\ 47,\ 113$$

besitzt, ein Teiler von $t^2 + 30u^2$ ist, und somit von der Form

$$15y^2 + 2z^2$$

sein muſs.

Einem andern, derselben Tafel entnommenen Beispiel zufolge kann man behaupten, daſs jede in einer der Formen

$$56x + 3,\ 5,\ 13,\ 19,\ 27,\ 45$$

enthaltene Primzahl ein Teiler von $t^2 + 14u^2$ ist, und somit von der Form

$$3y^2 + 4yz + 6z^2$$

sein muſs.

Der Beweis dieses Satzes ist oben für den Fall gegeben worden, wo c eine Primzahl oder das Doppelte einer Primzahl ist; derselbe kann aber auch ohne Schwierigkeit für jeden Wert von c geführt werden, wenn die Primzahl A von der Form $4cx + a$ gleichzeitig von der Form $4n + 3$ ist. Denn alsdann muſs notwendig die Zahl A in der Formel $t^2 + cu^2$ oder in der Formel $t^2 - cu^2$ aufgehen (No. 173). Sucht man aber die linearen Formen der Teiler von $t^2 - cu^2$, so stellen sich diese Formen als verschieden von den Formen der Teiler von $t^2 + cu^2$ heraus. Mithin kann die Zahl A, wenn sie von einer dieser letzteren Formen ist, kein Teiler von $t^2 - cu^2$ sein. Demnach

ist sie notwendig ein Teiler von $t^2 + cu^2$ und daher von einer der quadratischen Formen, welche diesen linearen Formen entsprechen.

Eine gleiche Schlufsfolgerung würde nicht mehr stattfinden, wenn A von der Form $4n + 1$ wäre; ja sie ist sogar unvollständig für den Fall $A = 4n + 3$, da sie die wirkliche Ermittlung der linearen Teiler sowohl der Formel $t^2 + cu^2$ wie der Formel $t^2 - cu^2$ voraussetzt. Deshalb ist es gut, einen andern Weg zum allgemeinen Beweise dieses Satzes einzuschlagen.

229.

Wir bemerken zunächst, dafs die lineare Form $4cx + a$, zu welcher die Primzahl A gehört, stets als eine von denjenigen betrachtet werden kann, welche einem quadratischen Teiler entsprechen. Ist

$$py^2 + 2qyz \pm rz^2$$

dieser Teiler, so kann man

$$py^2 + 2qyz \pm rz^2 = 4cx + a$$

setzen, oder, was dasselbe ist:

$$py^2 + 2qyz \pm rz^2 = 4cx + A.$$

Multipliciert man diese Gleichung mit p, so ergiebt sich:

$$(py + qz)^2 \pm cz^2 = 4pcx + pA,$$

und hieraus erkennt man, dafs $\frac{(py + qz)^2 - pA}{c}$ eine ganze Zahl ist. Demnach ist umsomehr, wenn ϑ ein Primfaktor von c ist, die Gleichung $\frac{x^2 - pA}{\vartheta} = e$ auflösbar, und daher ist:

$$\left(\frac{pA}{\vartheta}\right) = 1 \quad \text{oder} \quad \left(\frac{p}{\vartheta}\right)\left(\frac{A}{\vartheta}\right) = 1.$$

Nun ist aber allgemein $\left(\frac{p}{\vartheta}\right) = +1$ oder $= -1$, also $\left(\frac{p}{\vartheta}\right)\left(\frac{p}{\vartheta}\right) = 1$, und somit:

$$\left(\frac{A}{\vartheta}\right) = \left(\frac{p}{\vartheta}\right).$$

Wir könnten auch den speciellen Fall, wo $p = 1$, und den, wo p gleich einer Quadratzahl ist, betrachten, da man in diesen Fällen leicht beweisen kann, dafs A ein Teiler der gegebenen Formel $t^2 \pm cu^2$*) ist; indessen ist es besser, den Beweis in seiner ganzen Allgemeinheit zu verfolgen.

230.

Wir haben oben gesehen, dafs die Teiler von der Form $4n + 1$

*) Das doppelte Zeichen bedeutet nur, dafs die gegebene Formel $t^2 + cu^2$ oder $t^2 - cu^2$ sein kann; im Übrigen aber läfst dasselbe keine Unbestimmtheit übrig. Anm. d. Verf.

und die von der Form $4n+3$ durch ihnen eigentümliche quadratische Formen sich von einander unterscheiden; ja, wenn die gegebene Formel t^2+2au^2 ist, so zerfallen die Teiler sogar in vier Formen $8n+1$, $8n+3$, $8n+5$, $8n+7$, und diese sind in verschiedenen quadratischen Formen enthalten. Man kann daher annehmen, daſs der der linearen Form $4cx+a$ oder $4cx+A$ entsprechende quadratische Teiler $py^2+2qyz\pm 2mz^2$ nur Zahlen von derselben Art wie A enthält, d. h. solche Zahlen, daſs die Differenz zwischen diesen Zahlen und A durch 4 oder, falls die Formel t^2+2au^2 oder $2pm-q^2=2a$ ist, durch 8 teilbar ist. Mithin ist p, welches eine von diesen Zahlen ist, so beschaffen, daſs $\frac{p-A}{4}$ eine ganze Zahl, oder, falls $c=2a$, daſs $\frac{p-A}{8}$ eine solche ist.

Wir nehmen ferner an, daſs der Koefficient p eine Primzahl ist. Wäre er es nicht, so könnte man eine Primzahl suchen, welche in der Formel $py^2+2qyz\pm 2mz^2$ enthalten wäre. Ist diese Zahl:

$$p'=p\mu^2+2q\mu\nu\pm 2m\nu^2,$$

und bestimmt man μ^0 und ν^0 mittelst der Gleichung:

$$\mu\nu^0-\mu^0\nu=1,$$

so erhält man, wenn man

$$y=\mu y'+\mu^0 z', \qquad z=\nu y'+\nu^0 z'$$

setzt, als Transformation den quadratischen Teiler:

$$p'y'^2+2q'y'z'\pm 2m'z'^2,$$

in welchem der Koefficient des ersten Gliedes eine Primzahl ist. Betrachtet man also diese Vorbereitung als schon ausgeführt, so ist es gestattet, p als Primzahl anzunehmen.

Nehmen wir jetzt die bereits gefundene Gleichung

$$\left(\frac{A}{\vartheta}\right)=\left(\frac{p}{\vartheta}\right),$$

in welcher ϑ irgend einen Primfaktor von c bezeichnet, wieder auf, und sind $\alpha, \alpha', \alpha'', \ldots$ die Primteiler von der Form $4n+1$ und $\beta, \beta', \beta'', \ldots$ die Primteiler von der Form $4n+3$, so erhalten wir, wenn wir diese Zahlen für ϑ setzen:

$$\left(\frac{A}{\alpha}\right)=\left(\frac{p}{\alpha}\right), \quad \left(\frac{A}{\alpha'}\right)=\left(\frac{p}{\alpha'}\right), \quad \left(\frac{A}{\alpha''}\right)=\left(\frac{p}{\alpha''}\right), \ldots$$
$$\left(\frac{A}{\beta}\right)=\left(\frac{p}{\beta}\right), \quad \left(\frac{A}{\beta'}\right)=\left(\frac{p}{\beta'}\right), \quad \left(\frac{A}{\beta''}\right)=\left(\frac{p}{\beta''}\right), \ldots$$

Hieraus ergiebt sich nach dem Reciprocitätsgesetze und weil A und p entweder alle beide von der Form $4n+1$ oder alle beide von der Form $4n+3$ sind:

$$\left(\frac{\alpha}{A}\right) = \left(\frac{\alpha}{p}\right), \quad \left(\frac{\alpha'}{A}\right) = \left(\frac{\alpha'}{p}\right), \quad \left(\frac{\alpha''}{A}\right) = \left(\frac{\alpha''}{p}\right), \ldots$$

$$\left(\frac{\beta}{A}\right) = \left(\frac{\beta}{p}\right), \quad \left(\frac{\beta'}{A}\right) = \left(\frac{\beta'}{p}\right), \quad \left(\frac{\beta''}{A}\right) = \left(\frac{\beta''}{p}\right), \ldots$$

1) Ist demnach c ungerade, so ist c gleich dem Produkte aller Primzahlen $\alpha, \alpha', \alpha'', \ldots \beta, \beta', \beta'' \ldots$, und man erhält:

$$\left(\frac{c}{A}\right) = \left(\frac{\alpha}{A}\right)\left(\frac{\alpha'}{A}\right)\left(\frac{\alpha''}{A}\right) \cdots \left(\frac{\beta}{A}\right)\left(\frac{\beta'}{A}\right)\left(\frac{\beta''}{A}\right) \cdots$$

$$\left(\frac{c}{p}\right) = \left(\frac{\alpha}{p}\right)\left(\frac{\alpha'}{p}\right)\left(\frac{\alpha''}{p}\right) \cdots \left(\frac{\beta}{p}\right)\left(\frac{\beta'}{p}\right)\left(\frac{\beta''}{p}\right) \cdots$$

Da nun die Faktoren dieser Ausdrücke einander entsprechend gleich sind, so ist:

$$\left(\frac{c}{A}\right) = \left(\frac{c}{p}\right).$$

2) Ist c gerade, so enthält c aufser den vorhergehenden Faktoren den Faktor 2. Da jedoch p und A in Bezug auf die Vielfachen von 8 von derselben Form sind, so hat man $\left(\frac{2}{A}\right) = \left(\frac{2}{p}\right)$, und demnach ebenfalls:

$$\left(\frac{c}{A}\right) = \left(\frac{c}{p}\right).$$

Da aber p ein Teiler von $q^2 \pm c$ ist, so ist $\left(\frac{\mp c}{p}\right) = 1$; mithin ist auch $\left(\frac{\mp c}{A}\right) = 1$; folglich ist die Primzahl A jederzeit Teiler der gegebenen Formel $t^2 \pm cu^2$. Sie mufs somit von einer der quadratischen Formen sein, welche der linearen Form $4cx + a$ entsprechen.

231.

Der soeben bewiesene Satz ist unstreitig einer der **allgemeinsten** und **wichtigsten** Sätze der Zahlentheorie. Der Beweis, den wir dafür gegeben haben, setzt nur voraus, dafs es eine in dem quadratischen Teiler $py^2 + 2qyz + rz^2$ enthaltene Primzahl giebt. Diese Annahme ist aber nicht nur mit grofser Wahrscheinlichkeit richtig, man findet sie leicht bei allen in unsern Tafeln enthaltenen quadratischen Formen bestätigt; ja es unterliegt sogar keinem Zweifel, dafs die Formel $py^2 + 2qyz + rz^2$ unendlich viele Primzahlen enthält, aufser in dem Falle, wo die drei Zahlen p, q, r einen gemeinsamen Teiler ϑ besitzen. Einen solchen können sie indessen nicht haben, da wir angenommen haben, dafs c oder $pr - q^2$ keinen quadratischen Faktor besitze.

Nichtsdestoweniger könnte man den Beweis vollkommen unabhängig von der Voraussetzung machen, dafs p eine Primzahl ist.

Man müfste dazu verschiedene Fälle untersuchen, je nach der Anzahl der Faktoren, aus denen c zusammengesetzt ist.

Wir haben bereits den Fall untersucht, wo c eine Primzahl oder das Doppelte einer Primzahl ist. Nehmen wir also jetzt $c = \alpha . \beta$ an, wo α und β zwei beliebige ungerade Primzahlen sind. Zu gleicher Zeit sei

$$py^2 + 2qyz + 2mz^2$$

die quadratische Form, welche der linearen Form

$$4cx + a \text{ oder } 4cx + A$$

entspricht, so dafs p und A entweder alle beide von der Form $4n + 1$ oder alle beide von der Form $4n + 3$ sind. Alsdann hat man der Annahme nach:

$$py^2 + 2qyz + 2mz^2 = 4cx + A,$$

und wenn man mit p multipliciert:

$$(py + qz)^2 + cz^2 = 4cpx + Ap.$$

(Wir betrachten hier nur den Fall, wo c positiv ist, da der Fall, wo c negativ ist, in ähnlicher Weise behandelt werden kann).

Da nun $c = \alpha\beta$, so hat man in Bezug auf α und β die Gleichungen $\left(\frac{Ap}{\alpha}\right) = 1$, $\left(\frac{Ap}{\beta}\right) = 1$, und diese geben:

$$\left(\frac{A}{\alpha}\right) = \left(\frac{p}{\alpha}\right), \quad \left(\frac{A}{\beta}\right) = \left(\frac{p}{\beta}\right).$$

Es sei jetzt $p = \pi\pi'\pi''\pi'''\ldots$, wo $\pi, \pi'', \pi^{IV} \ldots$ Primzahlen von der Form $4n + 1$ und $\pi', \pi''', \ldots$ Primzahlen von der Form $4n + 3$ seien. Hätte p quadratische Faktoren, so könnte man dieselben ganz und gar weglassen und nur die ungleichen Faktoren beibehalten. Man hat also:

$$\left(\frac{A}{\alpha}\right) = \left(\frac{\pi}{\alpha}\right) \cdot \left(\frac{\pi'}{\alpha}\right) \cdot \left(\frac{\pi''}{\alpha}\right) \cdots$$

$$\left(\frac{A}{\beta}\right) = \left(\frac{\pi}{\beta}\right) \cdot \left(\frac{\pi'}{\beta}\right) \cdot \left(\frac{\pi''}{\beta}\right) \cdots$$

Die Gleichung $2pm - q^2 = c = \alpha\beta$ giebt aber:

$$\left(\frac{-\alpha\beta}{\pi}\right) = 1, \quad \left(\frac{-\alpha\beta}{\pi'}\right) = 1, \quad \left(\frac{-\alpha\beta}{\pi''}\right) = 1, \cdots$$

und ebenso für jeden andern Faktor von p. Folglich erhält man:

$$\left(\frac{\alpha}{\pi}\right) = \left(\frac{\beta}{\pi}\right), \quad \left(\frac{\alpha}{\pi''}\right) = \left(\frac{\beta}{\pi''}\right), \quad \left(\frac{\alpha}{\pi^{IV}}\right) = \left(\frac{\beta}{\pi^{IV}}\right), \cdots$$

$$\left(\frac{\alpha}{\pi'}\right) = -\left(\frac{\beta}{\pi'}\right), \quad \left(\frac{\alpha}{\pi'''}\right) = -\left(\frac{\beta}{\pi'''}\right), \cdots$$

Hieraus ergiebt sich nach dem Reciprocitätsgesetze (No. 166):

$$\left(\frac{\pi}{\alpha}\right) = \left(\frac{\pi}{\beta}\right), \qquad \left(\frac{\pi'}{\alpha}\right) = (-1)^{\frac{\alpha+\beta}{2}} \left(\frac{\pi'}{\beta}\right)$$

$$\left(\frac{\pi''}{\alpha}\right) = \left(\frac{\pi''}{\beta}\right), \qquad \left(\frac{\pi'''}{\alpha}\right) = (-1)^{\frac{\alpha+\beta}{2}} \left(\frac{\pi'''}{\beta}\right)$$

$$\left(\frac{\pi^{IV}}{\alpha}\right) = \left(\frac{\pi^{IV}}{\beta}\right),$$

$$\cdots\cdots \qquad \cdots\cdots\cdots$$

Nur die rechts stehenden Gleichungen bedürfen einiger Erläuterung. Das allgemeine Gesetz giebt:

$$\left(\frac{\pi'}{\alpha}\right) = (-1)^{\frac{\pi-1}{2}\cdot\frac{\alpha-1}{2}} \left(\frac{\alpha}{\pi'}\right),$$

und da $\frac{\pi'-1}{2}$ ungerade ist, so geht diese Gleichung über in:

$$\left(\frac{\pi'}{\alpha}\right) = (-1)^{\frac{\alpha-1}{2}} \left(\frac{\alpha}{\pi'}\right).$$

Ebenso hat man:

$$\left(\frac{\pi'}{\beta}\right) = (-1)^{\frac{\beta-1}{2}} \left(\frac{\beta}{\pi'}\right).$$

Da nun $\left(\frac{\alpha}{\pi'}\right) = -\left(\frac{\beta}{\pi'}\right)$ ist, so folgt hieraus:

$$\left(\frac{\pi'}{\alpha}\right) = (-1)^{\frac{\alpha+\beta}{2}} \left(\frac{\pi'}{\beta}\right),$$

und ebenso die andern auf π''', $\pi^{V}\ldots$ bezüglichen Gleichungen.

Multipliciert man die beiden vorstehenden Reihen von Gleichungen mit einander, so erhält man:

$$\left(\frac{p}{\alpha}\right) = (-1)^{\frac{\alpha+\beta}{2}\cdot k} \left(\frac{p}{\beta}\right),$$

wobei k die Anzahl der Faktoren π', π''', ..., welche von der Form $4n+3$ sind, bedeutet.

Ist zunächst A und somit p von der Form $4n+1$, so mufs die Zahl k gerade sein, und demnach ist

$$\left(\frac{p}{\alpha}\right) = \left(\frac{p}{\beta}\right), \text{ also auch } \left(\frac{A}{\alpha}\right) = \left(\frac{A}{\beta}\right).$$

Umgekehrt folgt hieraus

$$\left(\frac{\alpha}{A}\right) = \left(\frac{\beta}{A}\right), \text{ oder } \left(\frac{\alpha\beta}{A}\right) = +1.$$

Somit ist A ein Teiler von $t^2 + \alpha\beta u^2$.

Ist zweitens A sowohl wie p von der Form $4n+3$, so ist die Zahl k ungerade, und es ist:

$$\left(\frac{p}{\alpha}\right) = (-1)^{\frac{\alpha+\beta}{2}} \left(\frac{p}{\beta}\right),$$

folglich:
$$\left(\frac{A}{\alpha}\right) = (-1)^{\frac{\alpha+\beta}{2}} \left(\frac{A}{\beta}\right).$$
Hieraus ergiebt sich nach dem Reciprocitätsgesetze:
$$(-1)^{\frac{\alpha-1}{2}} \left(\frac{\alpha}{A}\right) = (-1)^{\frac{\alpha+\beta}{2} + \frac{\beta-1}{2}} \left(\frac{\beta}{A}\right),$$
und dies reduciert sich auf:
$$\left(\frac{\alpha}{A}\right) = (-1)^{\beta} \left(\frac{\beta}{A}\right).$$
oder:
$$\left(\frac{\alpha}{A}\right) = -\left(\frac{\beta}{A}\right).$$
Mithin ist:
$$\left(\frac{-\alpha\beta}{A}\right) = 1,$$
und daher A ebenfalls ein Teiler von $t^2 + \alpha\beta u^2$.

Der Schlufs, dafs A ein Teiler von $t^2 + cu^2$ sei, ist also richtig, wie beschaffen auch der Koefficient p sein möge, und es unterliegt keinem Zweifel, dafs er ebenfalls gelten würde, wenn c das Produkt von mehr als zwei Primzahlen wäre.

232.

Man erkennt nunmehr, dafs jeder Teil unsrer Tafeln mehrere **Sätze** liefert, welche **Beziehungen** zwischen den **linearen** Formen der Primzahlen und ihren **quadratischen** Formen ergeben. Die bemerkenswertesten von diesen Sätzen, oder diejenigen, welche sich auf die einfachsten Formeln beziehen, sind folgende:

Aus Tafel III.

1) Jede Primzahl von der Form $8x + 1$ oder $8x + 7$ ist von der Form $y^2 - 2z^2$.

2) Jede Primzahl von der Form $12x + 1$ ist von der Form $y^2 - 3z^2$, und jede Primzahl von der Form $12x + 11$ ist von der Form $3y^2 - z^2$.

3) Jede Primzahl von einer der Formen $20x + 1, 9, 11, 19$ ist von der Form $y^2 - 5z^2$.

4) Jede Primzahl von der Form $24x + 1$ oder $24x + 19$ ist von der Form $y^2 - 6z^2$, und jede Primzahl von der Form $24x + 5$ oder $24x + 23$ ist von der Form $6y^2 - z^2$.

5) Jede Primzahl von einer der Formen $28x + 1, 9, 25$ ist von der Form $y^2 - 7z^2$, und jede Primzahl von der Form $28x + 3, 19, 27$ ist von der Form $7y^2 - z^2$.

6) Jede Primzahl von einer der Formen $40x + 1, 9, 31, 39$ ist von der Form $y^2 - 10z^2$, und jede Primzahl von einer der Formen $40x + 3, 13, 27, 37$ ist von der Form $2y^2 - 5z^2$.

7) u. s. w.

Aus Tafel IV.

1) Jede Primzahl von der Form $4x + 1$ ist von der Form $y^2 + z^2$.

2) Jede Primzahl von der Form $20x + 1$ oder $20x + 9$ ist von der Form $y^2 + 5z^2$, und jede Primzahl von der Form $20x + 3$ oder $20x + 7$ ist von der Form $2y^2 + 2yz + 3z^2$.

3) Jede Primzahl von einer der Formen $52x + 1, 9, 17, 25, 29, 49$ ist von der Form $y^2 + 13z^2$, und jede Primzahl von einer der Formen $52x + 7, 11, 15, 19, 31, 47$ ist von der Form $2y^2 + 2yz + 7z^2$.

4) u. s. w.

Aus Tafel V.

1) Jede Primzahl von der Form $6x + 1$ ist von der Form $y^2 + yz + z^2$ oder, was auf dasselbe hinauskommt, von der Form $y^2 + 3z^2$.

2) Jede Primzahl von einer der Formen $14x + 1, 9, 11$ ist von der Form $y^2 + 7z^2$.

8) Jede Primzahl von einer der Formen $22x + 1, 3, 5, 9, 15$ ist von der Form $y^2 + yz + 3z^2$.

4) Jede Primzahl von der Form $30x + 1$ oder $30x + 19$ ist von der Form $y^2 + 15z^2$, und jede Primzahl von der Form $30x + 17$ oder $30x + 23$ ist von der Form $3y^2 + 5z^2$.

5) u. s. w.

Aus Tafel VI.

1) Jede Primzahl von der Form $8x + 1$ oder $8x + 3$ ist von der Form $y^2 + 2z^2$.

2) Jede Primzahl von einer der Formen $40x + 1, 9, 11, 19$ ist von der Form $y^2 + 10z^2$, und jede Primzahl von einer der Formen $40x + 7, 13, 23, 37$ ist von der Form $2y^2 + 5z^2$.

3) Jede Primzahl von einer der Formen $104x + 1, 3, 9, 17, 25, 27, 35, 43, 49, 51, 75, 81$ ist von einer der Formen $y^2 + 26z^2$ und $3y^2 + 2yz + 9z^2$, und jede Primzahl von einer der Formen $104x + 5, 7, 15, 21, 31, 37, 45, 47, 63, 71, 85, 93$ ist von einer der Formen $2y^2 + 13z^2$ und $6y^2 + 4yz + 5z^2$.

4) u. s. w.

Aus Tafel VII.

1) Jede Primzahl von der Form $24x + 5$ oder $24x + 11$ ist

von der Form $2y^2 + 3z^2$, und jede Primzahl von der Form $24x + 1$ oder $24x + 7$ ist von der Form $y^2 + 6z^2$.

2) Jede Primzahl von einer der Formen $56x + 3$, 5, 13, 19, 27, 45 ist von der Form $3y^2 + 2yz + 5z^2$, und jede Primzahl von einer der Formen $56x + 1$, 9, 15, 23, 25, 39 ist von einer der beiden Formen $y^2 + 14z^2$ und $2y^2 + 7z^2$.

3) Jede Primzahl von einer der Formen $88x + 13$, 19, 21, 29, 35, 43, 51, 61, 83, 85 ist von der Form $2y^2 + 11z^2$, und jede Primzahl von einer der Formen $88x + 1$, 9, 15, 23, 25, 31, 47, 49, 71, 81 ist von der Form $y^2 + 22z^2$.

4) Jede Primzahl von einer der Formen $120x + 11$, 29, 59, 101 ist von der Form $5y^2 + 6z^2$.

Jede Primzahl von einer der Formen $120x + 13$, 37, 43, 67 ist von der Form $10y^2 + 3z^2$.

Jede Primzahl von einer der Formen $120x + 1$, 31, 49, 79 ist von der Form $y^2 + 30z^2$.

Jede Primzahl von einer der Formen $120x + 17$, 23, 47, 113 ist von der Form $2y^2 + 15z^2$.

5) u. s. w. u. s. w.

Lagrange war der erste, welcher den Weg zur Entdeckung derartiger Sätze bahnte (man sehe die Abhandlungen der Berliner Akademie vom Jahre 1775). Indessen sind die Methoden, deren sich dieser bedeutende Mathematiker bediente, nur in sehr wenigen Fällen auf die Primzahlen von der Form $4n + 1$ anwendbar. Die in Bezug auf diese sich darbietende Schwierigkeit kann nur mit Hülfe des Reciprocitätsgesetzes, welches ich zuerst in den Abhandlungen der Pariser Akademie der Wissenschaften vom Jahre 1785 angegeben habe, vollständig beseitigt werden.

§ 13.

Andere Sätze, die quadratischen Formen der Zahlen betreffend.

233.

Ist P irgend eine Zahl, welche in der Formel $t^2 \pm cu^2$ aufgeht, und als solche in dem quadratischen Teiler $py^2 + 2qyz \pm rz^2$ enthalten, so kann man

$$P = p\alpha^2 + 2q\alpha\beta \pm r\beta^2$$

setzen. Bestimmt man sodann zwei Zahlen α^0, β^0 der Gleichung $\alpha\beta^0 - \beta\alpha^0 = 1$ gemäfs, und setzt man $\alpha y + \alpha^0 z$ und $\beta y + \beta^0 z$ an Stelle von y und z, so geht der quadratische Teiler

$$py^2 + 2qyz \pm rz^2$$

über in die Form

$$Py^2 + 2Qyz + Rz^2.$$

Ist P' ein andrer Teiler, der in derselben Formel $py^2 + 2qyz \pm rz^2$ oder in der ihr äquivalenten $Py^2 + 2Qyz \pm Rz^2$ enthalten ist, so kann man

$$P' = P\mu^2 + 2Q\mu\nu + R\nu^2$$

setzen, und dies giebt:

$$PP' = (P\mu + Q\nu)^2 \pm c\nu^2.$$

Mithin:

Sind P und P' zwei Teiler der Formel $t^2 \pm cu^2$, welche alle beide in einer und derselben quadratischen Formel $py^2 + 2qyz \pm rz^2$ enthalten sind, so ist ihr Produkt PP' stets von der Form $t^2 \pm cu^2$.

Sind umgekehrt die beiden Zahlen P und P' so beschaffen, dafs $PP' = t^2 \pm cu^2$ ist, wo t und u prim zu einander sind, so behaupte ich, dafs diese beiden Zahlen zu demselben quadratischen Teiler gehören.

Da nämlich t und u prim zu einander sind, so müssen es u und P ebenfalls sein; man kann also setzen: $t = Py + Qu$, wo y und Q unbestimmte Gröfsen sind. Dies giebt:

$$P' = Py^2 + 2Qyu + \frac{Q^2 \pm c}{P} u^2.$$

Da in diesem Ausdrucke u und P keinen gemeinschaftlichen Teiler haben, so sieht man, dafs $Q^2 \pm c$ durch P teilbar sein mufs. Setzt man also $Q^2 \pm c = PR$, so erhält man:

$$P' = Py^2 + 2Qyu + Ru^2.$$

Betrachtet man y und u als unbestimmte Gröfsen, so stellt die rechte Seite einen der quadratischen Teiler der Formel $t^2 \pm cu^2$ dar, und es ist klar, dafs dieser Teiler zugleich P und P' enthält. Wenn also die beiden Zahlen P und P' so beschaffen sind, u. s. w.

234.

Jede **Primzahl** A, welche in der Formel $t^2 \pm cu^2$ aufgeht, kann nur zu **einem** einzigen quadratischen Teiler dieser Formel gehören.

Denn wenn die Primzahl A zu zwei verschiedenen quadratischen Teilern gehörte, so könnte man diese in zwei andere transformieren, in denen A der Koefficient des ersten Gliedes wäre (No. 233). Sind

$$Ay^2 + 2B\,yz + C\,z^2$$
$$Ay^2 + 2B'yz + C'z^2$$

diese beiden Teiler, so kann man gleichzeitig $A > 2B$ und $> 2B'$ annehmen; denn wenn $2B > A$ wäre, so müfste man $y - mz$ für y setzen und m derart bestimmen, dafs der Koefficient von yz nicht gröfser als A wäre. Nachdem dieses festgestellt ist, hätte man stets:

$$B^2 - AC = B'^2 - AC' = \pm c;$$

mithin wäre $\frac{B^2 - B'^2}{A}$ eine ganze Zahl, und da A Primzahl ist, so müfste A in einem der Faktoren $B + B'$, $B - B'$ aufgehen. Da aber B und B' alle beide kleiner als $\frac{1}{2}A$, oder eins von ihnen höchstens gleich $\frac{1}{2}A$ ist, so sind die Zahlen $B + B'$ und $B - B'$ kleiner als A und daher ist weder der eine noch der andere Faktor durch A teilbar, wofern man nicht $B = B'$ annimmt. Alsdann aber sind die beiden in Rede stehenden quadratischen Teiler identisch; folglich kann die Primzahl A, welche in der Formel $t^2 \pm cu^2$ aufgeht, nur zu einem einzigen quadratischen Teiler dieser Formel gehören.

Bemerkung. Dieselbe Schlufsfolgerung würde gelten, wenn A das Doppelte einer Primzahl, und allgemein, wenn A irgend eine Potenz einer Primzahl oder das Doppelte dieser Potenz wäre. Denn die Gleichung $\frac{x^2 \pm c}{A} = e$ läfst nur eine einzige Lösung zu, wenn A von der erwähnten Form ist, oder allgemeiner, wenn $A = \alpha^n \vartheta$ oder $2\alpha^n \vartheta$ ist, wo ϑ einen durch α nicht teilbaren Teiler von c und α eine Primzahl bedeutet. (Siehe No. 193). Mithin kann in allen diesen Fällen, welche ziemlich umfassend sind, die Zahl A nur in einem einzigen quadratischen Teiler der Formel $t^2 \pm cu^2$ enthalten sein.

235.

Ist dagegen A eine **zusammengesetzte** Zahl, so kann es **mehrere** quadratische Teiler der Formel $t^2 \pm cu^2$ geben, welche die Zahl A enthalten.

Der quadratische Teiler nämlich, welcher A enthält, kann dargestellt werden durch die Formel $Ay^2 + 2Byz + Cz^2$, wo $2B < A$ und $B^2 - AC = \pm c$ ist. Da nun A bekannt ist, so kann man für B jede Zahl nehmen, welche der Gleichung $\frac{x^2 \pm c}{A} = e$ genügt, vorausgesetzt, dafs diese Lösung zwischen 0 und $\frac{1}{2}A$ liegt. Wenn ferner A ungleiche und mit c keine gemeinsamen Primfaktoren hat, so besitzt diese Gleichung, wie wir bereits in No. 193 gesehen haben,

2^{i-1} Lösungen, wobei i die Anzahl dieser Faktoren (aufser 2) angiebt. Mithin giebt es ebenfalls 2^{i-1} quadratische Teiler

$$Ay^2 + 2Byz + Cz^2$$

oder Formen von quadratischen Teilern, welche A enthalten. Es kann jedoch vorkommen, dafs mehrere dieser Teiler, auf den einfachsten Ausdruck reduciert, nicht von einander verschieden sind, so dafs mit Rücksicht auf die angegebene Grenze die Anzahl der die Zahl A enthaltenden quadratischen Teiler zwar nicht gröfser als 2^{i-1}, wohl aber kleiner als 2^{i-1} sein kann. Dies ist um so augenscheinlicher, als die Anzahl der quadratischen Teiler einer und derselben Formel $t^2 \pm cu^2$ zuweilen sehr gering ist und sich manchmal auf einen oder zwei reduciert, während die Gröfse 2^{i-1}, welche die Anzahl der Werte von B darstellt, wenn man eine aus mehreren Faktoren zusammengesetzte Zahl A nimmt, so grofs werden kann als man will.

Bemerkung. Bis hierher haben wir die Teiler der beiden Formeln $t^2 + cu^2$ und $t^2 - cu^2$ unterschiedslos betrachtet; von nun an werden wir uns in diesem Paragraphen nur mit der **ersten** Formel $t^2 + cu^2$ und deren quadratischen Teilern beschäftigen.

236.

Jede Primzahl A, welche von der Form $y^2 + az^2$ ist, wo a eine **positive** Zahl bedeutet, kann nur ein **einziges Mal von dieser Form** sein, so dafs man also nicht gleichzeitig $A = f^2 + ag^2$ und $A = f'^2 + ag'^2$ haben kann, wo g' verschieden von g ist.

Nehmen wir an, dafs diese beiden Formen, falls es möglich wäre, gleichzeitig stattfänden, und dafs somit

$$f^2 + ag^2 = f'^2 + ag'^2,$$

oder

$$f^2 - f'^2 = a(g'^2 - g^2)$$

wäre, so müfste $f + f'$ durch einen Faktor von a und $f - f'$ durch einen andern Faktor teilbar sein. Ist also $a = mn$, wo m und n zwei unbestimmte Faktoren sind, so hat man:

$$f + f' = mh, \qquad f - f' = nk,$$

und daher:

$$hk = g'^2 - g^2.$$



Ist φ der gröfste gemeinschaftliche Teiler von h und $g' + g$, so kann man setzen:

$$h = \mu\varphi, \qquad g + g' = \nu\varphi,$$

so dafs man nur noch der Gleichung

$$\mu k = (g' - g)\nu$$

zu genügen hat. Da nun aber μ und ν prim zu einander sind, so mufs

$$k = \nu\psi, \qquad g' - g = \mu\psi$$

sein, wo ψ eine neue unbestimmte Gröfse darstellt. Hieraus folgt:

$$f = \frac{1}{2}(mh + nk) = \frac{1}{2}(m\mu\varphi + n\nu\psi)$$

$$g = \frac{1}{2}(\nu\varphi - \mu\psi).$$

Mithin ist:

$$f^2 + ag^2 \text{ oder } A = \frac{1}{4}(\mu^2 m + \nu^2 n)(m\varphi^2 + n\psi^2).$$

Da nun A eine Primzahl ist, so mufs der eine der beiden Faktoren auf der rechten Seite, z. B. $m\mu^2 + n\nu^2$, gleich 4 oder gleich 2 sein.

Ist zuerst $m\mu^2 + n\nu^2 = 2$, so kann man weder $\mu = 0$ noch $\nu = 0$ setzen, weil jede dieser beiden Annahmen die beiden Formen $f^2 + ag^2$ und $f'^2 + ag'^2$ identisch machen würde. Mithin besteht die einzige Art, dieser Gleichung zu genügen, darin, dafs man alle Zahlen m, n, μ, ν gleich der Einheit annimmt. Alsdann aber hätte man:

$$a = 1, \qquad f = \frac{1}{2}(\varphi + \psi), \qquad g = \frac{1}{2}(\varphi - \psi)$$

$$f' = \frac{1}{2}(\varphi - \psi), \qquad g' = \frac{1}{2}(\varphi + \psi),$$

und es würden somit $f^2 + ag^2$ und $f'^2 + ag'^2$ gegen unsre Annahme nur eine und dieselbe Form $\frac{1}{4}(\varphi + \psi)^2 + \frac{1}{4}(\varphi - \psi)^2$ darstellen.

Ist zweitens $m\mu^2 + n\nu^2 = 4$, so giebt es, da man ebenfalls weder $\mu = 0$ noch $\nu = 0$ setzen kann, nur zwei Arten, diese Gleichung zu befriedigen, die eine, wenn man $m = n = 2$, $\mu = \nu = 1$ setzt, die andere, wenn man $m = 1$, $n = 3$, $\mu = \nu = 1$ setzt. Der erste Fall ergäbe $A = 2\varphi^2 + 2\psi^2$; es würde somit A keine Primzahl sein.

Im zweiten Falle erhält man:

$$A = \varphi^2 + 3\psi^2, \qquad f = \frac{1}{2}(\varphi + 3\psi), \qquad g = \frac{1}{2}(\varphi - \psi).$$

Diese letzteren Werte können aber nur stattfinden, wenn φ und ψ entweder alle beide gerade, oder alle beide ungerade sind; bei jeder

dieser beiden Annahmen würde aber $\varphi^2 + 3\psi^2$ oder A durch 4 teilbar sein. Mithin kann die Primzahl A in keinem Falle auf zweierlei Weise durch dieselbe Formel $y^2 + az^2$ dargestellt werden.

Bemerkung. Wenn eine Zahl A auf zwei verschiedene Arten durch die Formel $y^2 + az^2$ dargestellt werden kann, so ist diese Zahl notwendig eine zusammengesetzte Zahl, deren beide Faktoren sogar nach der vorhergehenden Analyse sich bestimmen lassen. Es ist jedoch zu beachten, dafs dieser Satz nicht mehr richtig wäre, wenn a eine **negative** Zahl ist; denn nimmt man an, dafs die Gleichung $A = y^2 - az^2$ eine Lösung besitze, so besitzt dieselbe unendlich viele.

237.

Wir haben bereits Gelegenheit gehabt zu bemerken, dafs das Produkt der beiden ähnlichen Formeln $x^2 + ay^2$, $p^2 + aq^2$ eine ebensolche Formel giebt, welche in den beiden Formen sich darstellen läfst:

$$(px - aqy)^2 + a(py + qx)^2$$
$$(px + aqy)^2 + a(py - qx)^2.$$

Man kann sich hiervon durch die einfache Entwicklung der beiden Gröfsen überzeugen. Man kann jedoch die Form dieser Produkte auch direkt finden, wenn man beachtet, dafs die beiden Faktoren $x^2 + ay^2$ und $p^2 + aq^2$ gleichbedeutend sind mit den vier folgenden:

$$x + y\sqrt{-a},\quad x - y\sqrt{-a},\quad p + q\sqrt{-a},\quad p - q\sqrt{-a}.$$

Multipliciert man nun die beiden Faktoren $x + y\sqrt{-a}$ und $p + q\sqrt{-a}$ mit einander, so ist das Produkt gleich:

$$px - aqy + (py + qx)\sqrt{-a}.$$

Die beiden andern Faktoren ergeben ebenso als Produkt:

$$px - aqy - (py + qx)\sqrt{-a},$$

und das Produkt dieser Produkte ist:

$$(px - aqy)^2 + a(py + qx)^2.$$

Das Resultat würde dasselbe sein, wenn man das Zeichen von q änderte; mithin ist eine andere Form des Produkts:

$$(px + aqy)^2 + a(py - qx)^2.$$

Diese Formeln gelten, welches auch das Zeichen von a sein möge. Das Folgende setzt aber voraus, dafs a **positiv** sei.

238.

Wenn die Formel $x^2 + ay^2$ eine **zusammengesetzte** Zahl N darstellt, welche m-mal von der Form $x^2 + ay^2$ sein möge, und wenn $p^2 + aq^2$ eine Primzahl A darstellt, so sieht man nach der vorhergehenden Nummer, daſs das Produkt AN $2m$ Formen, ähnlich der Form $x^2 + ay^2$, annehmen kann, vorausgesetzt jedoch, daſs N nicht teilbar ist durch A. Man wird sogleich sehen, warum wir diese Einschränkung machen.

Wenn die Primzahl A von der Form $p^2 + aq^2$ ist, so ist das Quadrat der Zahl A einmal von der Form x^2 und einmal von der Form $x^2 + ay^2$, denn man hat nach den vorstehenden Formeln:

$$A^2 = (p^2 + aq^2)^2 \quad \text{und} \quad A^2 = (p^2 - aq^2)^2 + a(2pq)^2$$

Wenn demnach die zusammengesetzte Zahl N m-mal von der Form $x^2 + ay^2$ ist, und wenn die Primzahl A ebenfalls die Form $p^2 + aq^2$ besitzt, so wird das Produkt NA^2 $3m$ Formen von der Art wie $X^2 + aY^2$ annehmen können, und unter diesen giebt es $2m$ Formen, in denen X und Y keinen gemeinschaftlichen Teiler A haben, und m Formen, in denen sie einen solchen besitzen. Es wird dabei ebenfalls vorausgesetzt, daſs A kein Teiler ist von N.

Ist die Primzahl A immer von der Form $p^2 + aq^2$, so ist der Kubus von A zweimal von eben dieser Form; denn es ist A^2 von der Form $(p - aq)^2 + a(2pq)^2$, und multipliciert man diese Gröſse mit $(p^2 + aq^2)$, so ergeben sich die beiden Formen:

$$(p^3 - 3apq^2)^2 + a(3p^2q - aq^3)^2$$
$$(p^3 + apq^2)^2 + a(p^2q + aq^3)^2.$$

Wird die letztere durch $X^2 + aY^2$ dargestellt, so sieht man, daſs X und Y den gemeinschaftlichen Teiler A haben, und daſs sich diese Form auf $(pA)^2 + a(qA)^2$ reduciert, also auf dieselbe Form, als ob man einfach $p^2 + aq^2$ mit A^2 multipliciert hätte.

Allgemein, ist A eine Primzahl von der Form $p^2 + aq^2$, so kann man

$$A^n = P^2 + aQ^2$$

setzen und erhält zur Bestimmung von P und Q die Gleichung:

$$(p + q\sqrt{-a})^n = P + Q\sqrt{-a},$$

in welcher man nach Entwicklung der linken Seite die rationalen Teile sowohl wie die irrationalen Teile unter sich gleichzusetzen hat.

Nun ist aber auch $A^n = A^2 \cdot A^{n-2}$, so daſs man, wenn man

$$A^{n-2} = P'^2 + aQ'^2$$

setzt, einen neuen Wert von A^n erhält, welcher lautet:

$$(AP')^2 + a(AQ')^2.$$

Einen ähnlichen Wert folgert man aus $A^4 \cdot A^{n-4}$ u. s. w. Mithin giebt es ebenso viele verschiedene Formen $X^2 + aY^2$ für die Potenz A^n, als es in $1 + \frac{n}{2}$ Einheiten giebt; aber unter diesen Formen giebt es nur eine einzige, in welcher X und Y prim zu einander sind. In allen andern haben X und Y der Reihe nach A, A^2, A^3, ... als gemeinschaftlichen Teiler. Mithin ist der Wert von A^n:

wenn $n = 2$, einmal A^2 und einmal von der Form $X^2 + aY^2$
wenn $n = 3$, zweimal von der Form $X^2 + aY^2$
wenn $n = 4$, einmal A^4 und zweimal von der Form $X^2 + aY^2$
wenn $n = 5$ dreimal von der Form $X^2 + aY^2$
u. s. w.

Da jeder Faktor $X^2 + aY^2$, wenn man ihn mit einer Zahl von derselben Form multipliciert, zwei Resultate von eben dieser Form hervorbringt, während X^2 allein nur eines giebt, so kann man allgemein schliefsen, dafs das Produkt aus einer Formel $f^2 + ag^2$ und A^n $n + 1$ Formen von der Art wie $x^2 + ay^2$ annehmen kann, welche alle von einander verschieden sind, vorausgesetzt, dafs A nicht in $f^2 + ag^2$ aufgeht.

Wenn demnach $N = \alpha^n \beta^{n'} \gamma^{n''} \ldots$ ist, wo $\alpha, \beta, \gamma \ldots$ Primzahlen und sämtlich von der Form $p^2 + aq^2$ sind, so ist die Zahl N ebenso oftmal von der Form $x^2 + ay^2$, als das Produkt

$$\frac{1}{2}(n + 1)(n' + 1)(n'' + 1)(n''' + 1) \ldots$$

Einheiten enthält. Diese Zahl ist gleich der halben Anzahl der Teiler von N, oder gleich derjenigen, welche angiebt, auf wie viele Arten man die Zahl N in zwei Faktoren zerlegen kann.

In dem Falle, wo $(n + 1)(n' + 1) \cdots$ ungerade ist, würde das Resultat auch noch richtig sein, wenn man nur den übrigbleibenden Bruch $\frac{1}{2}$ für 1 rechnet.

Ist $a = 1$, oder ist die in Rede stehende Form $x^2 + y^2$, so kommen der Faktor 2 und seine Potenzen gar nicht in Betracht und ändern nicht die Anzahl der Formen des Produkts. Denn multipliciert man $x^2 + y^2$ mit 2, so erhält man nur ein Produkt von derselben Form, und dieses ist: $(x + y)^2 + (x - y)^2$.

239.

Um eine Anwendung der allgemeinen Formel zu geben,

betrachten wir die drei Zahlen 5, 13, 17, welche alle drei von der Form $p^2 + q^2$ sind. Man findet so:

1) Das Produkt $5 \cdot 13 \cdot 17$ ist $\frac{1}{2} \cdot 2 \cdot 2 \cdot 2$ oder viermal von der Form $p^2 + q^2$.

2) Das Produkt $5^2 \cdot 13$ ist $\frac{1}{2} \cdot 3 \cdot 2$ oder dreimal von derselben Form.

3) Das Produkt $5^2 \cdot 13^2 \cdot 17$ ist $\frac{1}{2} \cdot 3 \cdot 3 \cdot 2$ oder neunmal von dieser Form.

4) Das Produkt $5^4 \cdot 13^4$ ist $\frac{1}{2} \cdot 5 \cdot 5$ oder dreizehnmal die Summe zweier Quadrate. Alle diese Sätze sind leicht zu beweisen.

Das umgekehrte Problem, welches beim ersten Anblick sehr schwierig erscheinen könnte, löst sich sehr einfach, wenn man auf das bei der direkten Lösung gefundene Resultat achtet.

Es sei z. B. die Aufgabe gestellt, eine Zahl zu finden, welche dreifsigmal von der Form $p^2 + 2q^2$ ist. Die einfachsten Zahlen dieser Form sind die Primzahlen 3, 17, 19, 41, 43, ... Bezeichnet man diese durch $\alpha, \beta, \gamma, \ldots$ und die gesuchte Zahl durch $\alpha^n \beta^{n'} \gamma^{n''} \ldots$, so mufs man bewirken, dafs $30 = \frac{1}{2}(n+1)(n'+1)(n''+1)\ldots$ werde. Dazu zerlege man 60 in Faktoren, die Primzahlen sein können oder nicht, z. B in $3 \cdot 4 \cdot 5$, und vermindere jeden Faktor um eine Einheit. Dadurch erhält man 2, 3, 4 für die Werte von n, n', n''. Mithin ist $\alpha^2 \beta^3 \gamma^4$ eine der gesuchten Zahlen; es mufs also z. B. $3^4 \cdot 17^3 \cdot 19^2$ der Aufgabe Genüge leisten.

Diese Lösung ist von Fermat ohne Beweis in seinen Anmerkungen zum Diophant Seite 128 angegeben worden.

Der Satz in No. 236, von dem wir soeben verschiedene Anwendungen gegeben haben, enthält eine **wesentliche** und sehr **bemerkenswerte Eigenschaft** der **Primzahlen**; er läfst sich indessen noch bedeutend verallgemeinern, wie man aus den folgenden Sätzen erkennen wird.

240.

Jede in der Formel $my^2 + nz^2$, wo m und n positiv*)

*) Die Zahlen m und n müssen prim zu einander sein, da $mf^2 + ng^2$ gleich einer Primzahl ist. Man kann aber ferner noch voraussetzen, dafs m und n keinen quadratischen Faktor haben; denn wäre $m = m'\alpha^2$, so würde offenbar die Formel $my^2 + nz^2$ in $m'y^2 + nz^2$ enthalten sein. Anm. d. Verf.

sind, enthaltene Primzahl A läfst sich nicht auf zwei verschiedene Arten durch diese Formel ausdrücken, so dafs man, wenn $A = mf^2 + ng^2$ ist, nicht zu gleicher Zeit $A = mf'^2 + ng'^2$, wo g' von g verschieden ist, haben kann.

Hätte man gleichzeitig:

$$A = mf^2 + ng^2 = mf'^2 + ng'^2,$$

so würde hieraus folgen:

$$\frac{f^2 - f'^2}{n} = \frac{g'^2 - g^2}{m}.$$

In dieser Gleichung mufs jede Seite eine ganze Zahl sein, da m und n keinen gemeinschaftlichen Teiler haben. Ist daher $n = \alpha\beta$, $m = \gamma\delta$, so kann man allgemein setzen:

$$f + f' = \alpha MN, \qquad g' + g = \gamma MP$$
$$f - f' = \beta PQ, \qquad g' - g = \delta NQ,$$

und dies giebt:

$$2f = \alpha MN + \beta PQ$$
$$2g = \gamma MP - \delta NQ,$$

somit:

$$4mf^2 + 4ng^2 \text{ oder } 4A = (\alpha\gamma M^2 + \beta\delta Q^2)(\alpha\delta N^2 + \beta\gamma P^2).$$

Nun kann aber, da A eine Primzahl ist, diese Gleichung nur bestehen, wenn einer der Faktoren der rechten Seite gleich 4 oder gleich 2 ist.

Ist erstens $\alpha\gamma M^2 + \beta\delta Q^2 = 2$, so bemerke ich, dafs keine der Zahlen M, N, P, Q gleich 0 angenommen werden darf, weil durch diese Annahme die beiden Formen $mf^2 + ng^2$, $mf'^2 + ng'^2$ identisch werden würden. Man kann also der vorigen Gleichung nur genügen, wenn man $\alpha\beta\gamma\delta = 1$ und $M = Q = 1$ setzt. Alsdann aber würde die Zahl A von der Form $y^2 + z^2$ werden, und könnte dieselbe mithin nur einmal von dieser Form sein (No. 236).

Ist zweitens $\alpha\gamma M^2 + \beta\delta Q^2 = 4$, so kann diese Gleichung nur gelten, wenn man $\alpha\beta\gamma\delta = 3$ und $M = Q = 1$ setzt. Alsdann würde die Zahl A von der Form $y^2 + 3z^2$ sein, und dies käme wiederum auf den bereits in No. 236 untersuchten Fall zurück.

Mithin kann in allen Fällen die Primzahl A nur auf eine Weise durch die Formel $my^2 + nz^2$ dargestellt werden.

241.

Das Doppelte einer Primzahl A kann ebenfalls nicht auf zwei verschiedene Arten durch dieselbe Formel $my^2 + nz^2$

dargestellt werden, so dafs man, wenn $2A = mf^2 + ng^2$ ist, nicht zu gleicher Zeit $2A = mf'^2 + ng'^2$, wo g' von g verschieden ist, haben kann.

Denn bleibt alles wie beim vorhergehenden Satze, so gelangt man ebenso zu der Gleichung:

$$8A = (\alpha\gamma M^2 + \beta\delta Q^2)(\alpha\delta N^2 + \beta\gamma P^2).$$

Damit aber diese Gleichung bestehen könne, mufs einer der Faktoren der rechten Seite gleich 2, gleich 4, oder gleich 8 sein, ohne dafs jedoch eine der Zahlen M, N, P, Q gleich 0 wäre.

Ist erstens $\alpha\gamma M^2 + \beta\delta Q^2 = 2$, so kann diese Gleichung nur stattfinden, wenn $\alpha\beta\gamma\delta = 1$ und $M = Q = 1$ ist. Alsdann aber würde $2A$ von der Form $y^2 + z^2$ sein. Hätte man also:

$$2A = f^2 + g^2 = f'^2 + g'^2,$$

so erhielte man hieraus:

$$A = \left(\frac{f+g}{2}\right)^2 + \left(\frac{f-g}{2}\right)^2 = \left(\frac{f'+g'}{2}\right)^2 + \left(\frac{f'-g'}{2}\right)^2.$$

Mithin würde die Primzahl A zweimal von der Form $y^2 + z^2$ sein, was unmöglich ist (No. 236).

Ist zweitens $\alpha\gamma M^2 + \beta\delta Q^2 = 4$, so besteht die einzige Art, dieser Gleichung zu genügen (ohne dafs man M oder Q gleich 0 setzt oder $\alpha\beta\gamma\delta$ durch eine Quadratzahl teilbar annimmt), darin, dafs man $\alpha\beta\gamma\delta = 3$ und $M = Q = 1$ setzt. Alsdann aber hätte man $2A = f^2 + 3g^2$, eine Gleichung, welche unmöglich ist, da die linke Seite von der Form $4n + 2$ ist, während die rechte stets entweder ungerade oder ein Vielfaches von 4 ist.

Ist drittens $\alpha\gamma M^2 + \beta\delta Q^2 = 8$, so ist zunächst leicht zu sehen, dafs in diesem Falle $\alpha\beta\gamma\delta$ oder mn keine gerade Zahl sein kann; denn setzt man z. B. $\alpha\gamma = 2$, $\beta\delta = 3$, so würde man die Gleichung $2M^2 + 3N^2 = 8$ erhalten, welcher man nur dadurch genügen könnte, dafs man $N = 0$ setzt. Die andern geraden Werte von mn könnten nur 2 oder 10 sein; man würde aber ebenso erkennen, dafs sie unzulässig sind.

Es bleiben also nur die ungeraden Werte von mn oder $\alpha\beta\gamma\delta$ zu untersuchen, wenigstens diejenigen, für welche die Summe der beiden Faktoren $\alpha\gamma + \beta\delta$ nicht gröfser ist als 8; denn es ist die Gröfse $\alpha\gamma M^2 + \beta\delta Q^2$ wenigstens gleich dieser Summe, da man weder M noch Q gleich 0 setzen darf.

Da der Fall $mn = 1$ bereits untersucht ist, so sei $mn = 3$.

Dann erhält man $M^2 + 3Q^2 = 8$, eine Gleichung, deren Unmöglichkeit augenscheinlich ist.

Ist $mn = 5$, so erhält man $M^2 + 5Q^2 = 8$, eine Gleichung, die ebenfalls unmöglich ist.

Ist $mn = 7$, so erhält man $M^2 + 7Q^2 = 8$. Diese Gleichung ist zwar möglich, man erhielte aber dann $2A = f^2 + 7g^2$, und diese Gleichung ist unmöglich, weil die rechte Seite entweder ungerade oder ein Vielfaches von 8 ist.

Wegen des quadratischen Faktors darf man nicht $mn = 9$ setzen; ebenso wenig $mn = 11$ oder $mn = 13$, da $1 + 11$ und $1 + 13$ gröſser sind als 8.

Ist endlich $mn = 15$, und $\alpha\gamma = 3$, $\beta\delta = 5$, so ist die Gleichung $3M^2 + 5Q^2 = 8$ möglich. Alsdann aber hätte man $2A = f^2 + 15g^2$ oder $2A = 3f^2 + 5g^2$, Gleichungen, welche alle beide unmöglich sind, da die rechte Seite entweder ungerade oder ein Vielfaches von 8 ist.

Mithin kann in keinem Falle das Doppelte einer Primzahl auf zweierlei Weisen in der Formel $my^2 + nz^2$ enthalten sein.

242.

Jede Primzahl P oder das Doppelte einer Primzahl, welche in der quadratischen Formel $py^2 + 2qyz + 2\pi z^2$ enthalten ist, kann nur auf eine Weise durch diese Formel ausgedrückt werden, so daſs, wenn man

$$P = pf^2 + 2qfg + 2\pi g^2$$

hat, nicht zu gleicher Zeit

$$P = pf'^2 + 2qf'g' + 2\pi g'^2$$

sein kann. (Man setzt stets voraus, daſs p ungerade und $2p\pi - q^2$ gleich einer positiven Zahl c sei.)

Wir bemerken zunächst, daſs der Fall, wo P das Doppelte einer Primzahl ist, leicht auf den Fall zurückgeführt werden kann, wo P eine Primzahl ist. Denn ist:

$$2A = pf^2 + 2qfg + 2\pi g^2$$
$$2A = pf'^2 + 2qf'g' + 2\pi g'^2,$$

so müssen f und f' gerade sein. Setzt man also $f = 2h$, $f' = 2h'$, so erhält man:

$$A = 2ph^2 + 2qhg + \pi g^2$$
$$A = 2ph'^2 + 2qh'g' + \pi g'^2.$$

Wenn es also unmöglich ist, daſs eine Primzahl A auf zweierlei Weisen in einer und derselben quadratischen Formel enthalten sei,



so ist es gleichfalls unmöglich, dafs das Doppelte $2A$ derselben durch die quadratische Formel, welche $2A$ enthält, auf zwei Arten ausgedrückt werden könne. Umgekehrt, wenn der Satz für den Fall $P = 2A$ bewiesen wäre, so würde er es auch für den Fall $P = A$ sein. Aus diesem Grunde reicht es hin, einen von diesen Fällen zu betrachten.

Es sei also A eine Primzahl, welche in der Eormel

$$py^2 + 2qyz + 2\pi z^2,$$

die man als einen der quadratischen Teiler der Formel $t^2 + cu^2$ ansehen kann, enthalten ist. Setzt man:

$$A = pf^2 + 2qfg + 2\pi g^2,$$

und substituiert man, nachdem man f^0 und g^0 der Gleichung

$$fg^0 - f^0 g = 1$$

gemäfs bestimmt hat, $fy + f^0 z$ und $gy + g^0 z$ an Stelle von y und z in die Formel $py^2 + 2qyz + 2\pi z^2$, so wird diese Formel von der Form:

$$Ay^2 + 2Byz + Cz^2,$$

wobei $AC - B^2 = c$ ist.

Wenn demnach die Zahl A auf zwei verschiedene Weisen in der gegebenen Formel $py^2 + 2qyz + 2\pi z^2$ enthalten wäre, so müfste man der Gleichung

$$A = Ay^2 + 2Byz + Cz^2$$

genügen können, ohne dafs man $z = 0$ setzt. Multipliciert man diese Gleichung mit A, so ergiebt sich:

$$A^2 = (Ay + Bz)^2 + cz^2,$$

oder:

$$A^2 - (Ay + Bz)^2 = cz^2.$$

Ist $c = mn$, wo m und n zwei unbestimmte Faktoren sind, so kann man setzen:

$$A + Ay + Bz = mM$$
$$A - Ay - Bz = nN,$$

wodurch die aufzulösende Gleichung übergeht in:

$$Mn = z^2.$$

Dieser Gleichung genügt man aber allgemein, wenn man

$$M = \lambda\mu^2, \quad N = \lambda\nu^2, \quad z = \lambda\mu\nu$$

setzt, wo μ und ν prim zu einander sind. Man erhält also:

$$A + Ay + B\lambda\mu\nu = m\lambda\mu^2$$
$$A - Ay - B\lambda\mu\nu = n\lambda\nu^2,$$

und hieraus folgt:

$$2A = \lambda(m\mu^2 + n\nu^2).$$

Dieses Resultat, welches gilt, wie beschaffen auch A sein möge, zeigt, dafs, wenn irgend eine Zahl A auf zwei verschiedene Arten in einer und derselben quadratischen Formel $py^2 + 2qyz + 2\pi z^2$ enthalten ist, das Doppelte $2A$ derselben das Produkt von zwei Faktoren λ, ω ist, von denen der eine ω die Form $my^2 + nz^2$ (wo $mn = c$) besitzt, der andere λ kleiner als $\frac{A}{\sqrt{c}}$ ist.

Ist jetzt A eine Primzahl, so kann man, weil man von dem Falle $c = 1$ absehen darf, weder $\lambda = A$ noch $\lambda = 2A$ setzen; mithin mufs, da λ ein Teiler von $2A$ ist, λ gleich 1 oder gleich 2 sein. Man erhält daher

$$\text{entweder } A = m\mu^2 + n\nu^2$$
$$\text{oder } 2A = m\mu^2 + n\nu^2.$$

Ist erstens $A = m\mu^2 + n\nu^2$, so ist die Primzahl A in der Formel $my^2 + nz^2$ enthalten, und diese ist einer der quadratischen Teiler der Formel $t^2 + cu^2$. Da jedoch eine und dieselbe Primzahl nicht zu zwei verschiedenen quadratischen Teilern derselben Formel $t^2 + cu^2$ gehören kann, so folgt daraus, dafs die Formel $my^2 + nz^2$ mit der gegebenen Formel $py^2 + 2qyz + 2\pi z^2$ zusammenfallen mufs. Nun haben wir aber (No. 240) bewiesen, dafs die Primzahl A nur einmal von der Form $my^2 + nz^2$ sein kann; mithin kann sie auch nur einmal die äquivalente Form $py^2 + 2qyz + 2\pi z^2$ besitzen.

Ist zweitens $2A = m\mu^2 + n\nu^2$, so gehört die Zahl $2A$ zu dem quadratischen Teiler $my^2 + nz^2$. Da jedoch die Zahl A in dem Teiler $py^2 + 2qyz + 2\pi z^2$ enthalten ist, so folgt, dafs $2A$ in dem konjugierten Teiler $2py^2 + 2qyz + \pi z^2$ enthalten ist. Da $2A$ nicht zu zwei verschiedenen quadratischen Teilern gehören kann, so mufs also die Formel $2py^2 + 2qyz + \pi z^2$ mit $my^2 + nz^2$ identisch sein. Wenn es aber zwei Lösungen der Gleichung

$$A = py^2 + 2qyz + 2\pi z^2$$

gäbe, so würde es auch zwei Lösungen der Gleichung

$$2A = 2py^2 + 2qyz + \pi z^2,$$

und somit auch zwei Lösungen der mit dieser identischen Gleichung $2A = my^2 + nz^2$ geben. Dies ist aber unmöglich (No. 241).

Demnach läfst sich die Primzahl A nicht auf zwei verschiedene Arten durch dieselbe Formel $py^2 + 2qyz + 2\pi z^2$ ausdrücken. Also „Jede Primzahl P u. s. w.“



243.

Bemerkung. Der vorhergehende Satz und auch die Sätze der No. 240 und 241 erleiden in drei Fällen eine **Ausnahme**, nämlich:

1) Wenn der quadratische Teiler von der Form

$$py^2 + 2pyz + 2\pi z^2 \text{ oder einfach } py^2 + rz^2$$

ist, was $q = 0$ voraussetzt.

2) Wenn er von der Form

$$py^2 + 2qyz + 2qz^2$$

ist, was $r = 2q$ voraussetzt.

3) Wenn er von der Form

$$py^2 + 2qyz + pz^2$$

ist, was $r = p$ voraussetzt.

Denn es ist ersichtlich, dafs in diesen verschiedenen Fällen jede Art, eine gegebene Zahl P durch einen von diesen Teilern darzustellen, unmittelbar eine zweite liefert.

1) Genügt man z. B. der Gleichung $P = py^2 + rz^2$, indem man $y = m$, $z = n$ setzt, so genügt man ihr ebenfalls, wenn man $y = m$ und $z = -n$ setzt, und dies ist, streng genommen, eine verschiedene Lösung.

2) Wird die Gleichung $P = py^2 + 2qyz + 2qz^2$ dadurch befriedigt, dafs man $y = m$ und $z = n$ setzt, so kann man ihr auch genügen, wenn man $y = m$ und $z = -m - n$ setzt.

3) Wird die Gleichung $P = py^2 + 2qyz + pz^2$ dadurch befriedigt, dafs man $y = m$ und $z = n$ setzt, so wird ihr auch genügt, wenn man $y = n$ und $z = m$ setzt.

Zur Abkürzung werden wir diejenigen quadratischen Teiler, welche zu einem dieser drei Fälle gehören, **ambige** (bifides) quadratische Teiler oder einfach **ambige Teiler** nennen; zugleich aber wollen wir festsetzen, dafs die **beiden** Lösungen, welche zusammengehören, und von denen die eine aus der andern in derselben Weise entsteht, nur als **eine** Lösung betrachtet werden sollen. Alsdann sind die vorhergehenden Sätze vollständig allgemein und sie erleiden keine Ausnahme.

244.

Jede Primzahl A, welche in der quadratischen Formel $py^2 + qyz + rz^2$, deren Koefficienten **ungerade** sind, enthalten ist, kann darin nur auf eine Weise enthalten sein, mit Ausnahme des selbstverständlichen Falles, wo zwei der Zahlen

p, q, r einander gleich sind. (Es wird stets vorausgesetzt, dafs $4pr - q^2$ gleich einer positiven Zahl c sei).

Wir haben bereits in No. 221 gesehen, dafs die Formel

$$py^2 + qyz + rz^2$$

die drei folgenden einschliefst:

$$py^2 + 2qyz + 4rz^2$$
$$4py^2 + 2qyz + rz^2$$
$$(p - q + r)y^2 + (4p - 2q)yz + 4pz^2.$$

Mithin mufs die Primzahl A zu einer von diesen Formeln gehören. Werden dieselben aber auf die gewöhnliche Form gebracht, in welcher zwei Koefficienten gerade sind, so folgt aus dem vorigen Satze, dafs die Zahl A nur auf eine einzige Weise in der Formel, zu welcher sie gehört, enthalten sein kann. Mithin kann sie nur auf eine Weise durch die gegebene Formel $py^2 + qyz + rz^2$ dargestellt werden, aufser im Falle der ambigen Teiler, von denen wir absehen.

Anmerkung. Die vorhergehenden Sätze, die sich auf die Zahlen $P = A$, $P = 2A$, welche entweder Primzahlen oder das Doppelte von Primzahlen sind, beziehen, finden in gleicher Weise Anwendung auf die Zahlen von der Form $P = A^k$, $P = 2A^k$, wo k ein beliebiger Exponent ist. Denn bei diesen Formen kann ebenso wie bei denen, wo $k = 1$ ist, die Zahl P nur zu einem einzigen quadratischen Teiler der Formel $t^2 + cu^2$ gehören (siehe No. 234).

245.

Es sei P eine **zusammengesetzte** Zahl, welche entweder ungerade oder das Doppelte einer ungeraden Zahl ist. Nimmt man an, dafs P ein Teiler der Formel $t^2 + cu^2$, und dafs somit P in einem oder mehreren quadratischen Teilern dieser Formel enthalten sei, so behaupte ich, dafs P durch diese quadratischen Teiler stets auf 2^{i-1} verschiedene Arten dargestellt werden kann, wo i die Anzahl der ungleichen Primfaktoren bedeutet, welche in P aber nicht in c aufgehen.

Da nämlich P ein Teiler der Formel $t^2 + cu^2$ ist, so ist es auch ein Teiler der Formel $x^2 + c$, und die Gleichung $\frac{x^2 + c}{P} = e$ besitzt so viele Lösungen, als 2^{i-1} Einheiten enthält (siehe No. 193). Sind Q, Q', Q'', ... diese verschiedenen Werte von x, welche kleiner als $\frac{1}{2}P$ sind, und sind zugleich R, R', R'', ... die entsprechenden Werte



von $\frac{x^2+c}{P}$, so kann man aus diesen Zahlen die Formeln bilden:

$$Py^2 + 2Qyz + Rz^2$$
$$Py^2 + 2Q'yz + R'z^2$$
$$Py^2 + 2Q''yz + R''z^2$$
u. s. w.,

in denen P beständig dasselbe ist, und die sämtlich quadratische Teiler der Formel $t^2 + cu^2$ sind.

Ist $py^2 + 2qyz + rz^2$ einer der Teiler dieser Formel, und zwar in seiner einfachsten Gestalt, und ist in diesem die Zahl P enthalten, so kann man also

$$P = pf^2 + 2qfg + rg^2$$

setzen. Bestimmt man sodann f^0 und g^0 der Gleichung $fg^0 - f^0g = 1$ gemäfs und setzt man $fy + f^0z$ an Stelle von y und $gy + g^0z$ an Stelle von z, so geht die Formel

$$py^2 + 2qyz + rz^2$$

durch diese Substitution über in

$$Py^2 + 2Myz + Nz^2,$$

und man erhält:

$$M = pff^0 + q(fg^0 + f^0g) + rgg^0$$
$$N = pf^{0\,2} + 2qf^0g^0 + rg^{0\,2}.$$

Ferner kann man immer f^0 und g^0 derart annehmen, dafs M kleiner oder nicht gröfser als $\frac{1}{2}P$ ist. Daraus erkennt man, dafs, wenn M nach und nach jeder der Zahlen Q, Q', Q'', ... gleich werden soll (und dies ist notwendig, da jeder quadratische Teiler

$$Py^2 + 2Qyz + Rz^2,$$

nachdem er auf die einfachste Form gebracht ist, mit einem der durch

$$py^2 + 2qyz + rz^2$$

dargestellten Teiler übereinstimmen mufs), die Werte von f und g sich auf ebenso viele Arten müssen ändern können, als es Zahlen Q, Q', Q'', ... giebt, d. h. auf 2^{i-1} Arten, wo i die Anzahl der ungleichen und ungeraden Primfaktoren ist, welche in P aber nicht in c aufgehen.

Mithin ist die Zahl P auf 2^{i-1} verschiedene Arten in den quadratischen Teilern der Formel $t^2 + cu^2$ enthalten.

246.

Wenn der quadratische Teiler $py^2 + 2qyz + rz^2$ nur allein zu einer und derselben Gruppe von linearen Teilern gehört, so müssen die 2^{i-1} Formen, von denen eben die Rede war, in diesem

einen Teiler enthalten sein; es giebt daher in diesem Falle 2^{i-1} verschiedene Arten, der Gleichung

$$P = py^2 + 2qyz + rz^2$$

zu genügen. Es ist dies ein **bemerkenswertes Resultat**, das verdient, an einem Beispiel bestätigt zu werden.

Die Formel $t^2 + 69u^2$ hat der Tafel IV zufolge die Primzahlen 5, 7, 13, 17, 19 ... zu Teilern; mithin ist z. B. das Produkt 5 . 7 . 17 oder 595 ein Teiler derselben Formel. Da dieser Teiler von der Form $276x + 43$ ist, so zeigt dieselbe Tafel, dafs er in dem quadratischen Teiler $7y^2 + 2yz + 10z^2$ enthalten sein mufs, und da dieser Teiler der einzige seiner Art ist, und zugleich die in ihm enthaltene Zahl 595 aus drei ungleichen, ungeraden Primfaktoren zusammengesetzt ist, so mufs dem vorhergehenden Satze zufolge 595 auf 2^{i-1} oder 4 Arten in der Formel $7y^2 + 2yz + 10z^2$ enthalten sein. In der That, bringt man die Gleichung

$$595 = 7y^2 + 2yz + 10z^2$$

auf die Form:

$$(7y + z)^2 = 4165 - 69z^2,$$

und giebt man z die aufeinanderfolgenden Werte 0, 1, 2, 3, ..., so findet man die folgenden Lösungen:

$$\begin{array}{lcl} z = 1 & , & y = 9 \\ \quad 6 & & \quad 5 \\ \quad 7 & \ldots & \begin{cases} \ \ 3 \\ -5. \end{cases} \end{array}$$

Es giebt also drei Werte von z, von denen einer zu zwei Werten von y gehört, und somit giebt es, übereinstimmend mit unserm Satze, vier Lösungen der gegebenen Gleichung.

Bemerkung 1. Dieselben Ausnahmen, die wir in No. 243 angegeben haben für den Fall, wo P eine Primzahl oder das Doppelte einer Primzahl ist, finden in gleicher Weise statt, wenn P eine zusammengesetzte Zahl ist. Sie beziehen sich indessen alle auf die ambigen Teiler, so dafs man von ihnen absehen kann.

Bemerkung 2. Wenn eine ungerade Zahl P Teiler der Formel $t^2 + cu^2$ ist, in welcher c von der Form $8n + 3$ ist, und wenn somit P in dem quadratischen Teiler $py^2 + qyz + rz^2$, dessen Koefficienten ungerade sind, enthalten ist, so beweist man wie oben, dafs die Zahl P auf 2^{i-1} verschiedene Arten in den quadratischen Teilern der Formel $t^2 + cu^2$ enthalten ist, wobei i die Anzahl der ungleichen Primfaktoren, welche in P aber nicht in c aufgehen, bedeutet.



Hiervon giebt es keine Ausnahme, auch nicht, wenn $r = q$ wäre, vorausgesetzt, dafs man die Lösung $y = m$, $z = n$ der Gleichung

$$P = py^2 + qyz + qz^2$$

als nicht verschieden von der Lösung $y = m$, $z = -m - n$ betrachtet.

247.

Ist c eine Primzahl oder das Doppelte einer Primzahl, so kann jede in einem quadratischen Teiler der Formel $t^2 + cu^2$ enthaltene Zahl N nur auf eine Weise darin enthalten sein, so lange nicht $N > \frac{3}{2}c$ ist.

Zum Beweise suchen wir die Bedingungen dafür, dafs die Zahl N zweimal in dem quadratischen Teiler $py^2 + 2qyz + rz^2$ enthalten sei. Alsdann würde man, wenn man $py + qz = x$ setzt, die beiden Lösungen erhalten:

$$pN = x^2 + cz^2 = x'^2 + cz'^2.$$

1) Ist $z' = z$, so kann man nicht zugleich $x' = x$ setzen, da alsdann $y' = y$ sein und die beiden Lösungen nur eine ausmachen würden. Man kann jedoch $x' = -x$ setzen und dies giebt:

$$p(y + y') + 2qz = 0.$$

Da die Zahl $c = pr - q^2$ eine Primzahl oder das Doppelte einer Primzahl ist, so werden die Zahlen p und $2q$ prim zu einander sein oder nur 2 zum gemeinsamen Teiler haben.

Im ersten Falle kann man der Gleichung

$$p(y + y') + 2qz = 0$$

nur dadurch genügen, dafs man

$$y + y' = 2mq, \quad z = -mp$$

setzt. Man hat also dann:

$$N = py^2 - 2qmpy + rm^2p^2 = p\left[(y - mq)^2 + cm^2\right];$$

folglich:

$$N > pcm^2,$$

oder allgemein:

$$N > pc.$$

Da die Fälle $p = 1$ und $p = 3$ nur eine und dieselbe Lösung geben, so ist wenigstens $p = 5$. Damit demnach N zweimal in demselben quadratischen Teiler enthalten sei, mufs $N > 5c$ sein.

In dem zweiten Falle, in welchem p gerade ist, erhält man, wenn man $p = 2\pi$ setzt, die Gleichung

$$\pi(y + y') + qz = 0.$$

Man genügt derselben allgemein, wenn man

$$z = -\pi m, \quad y + y' = qm$$

setzt. Daraus folgt:

$$N = 2\pi y^2 - 2q\pi y m + r\pi^2 m^2 = \frac{\pi}{2}\left[(2y - qm)^2 + cm^2\right];$$

mithin:

$$N > \frac{\pi}{2} cm,$$

oder allgemein:

$$N > \frac{pc}{4}.$$

Da man weder $p = 2$ noch $p = 4$ setzen kann, weil sich hieraus an und für sich keine zwei Lösungen ergeben, so ist der kleinste Wert, welchen p haben kann, gleich 6, und dies giebt $N > \frac{3}{2}c$.

2) Ist $z' > z$, so mufs, weil alsdann $x^2 - x'^2 = c(z'^2 - z^2)$ ist, einer der beiden Faktoren $x + x'$, $x - x'$ der linken Seite durch c teilbar sein, und da das Vorzeichen von x' beliebig ist, so kann man $x + x' = cu$ setzen. Daraus folgt:

$$x - x' = \frac{z'^2 - z^2}{u}, \quad x = \frac{1}{2}cu + \frac{z'^2 - z^2}{2u}$$

und:

$$Np = \frac{1}{4}c^2u^2 + \frac{c}{2}(z'^2 + z^2) + \left(\frac{z'^2 - z^2}{2u}\right)^2.$$

Mithin ist:

$$Np > \frac{1}{4}c^2u^2,$$

oder allgemein:

$$Np > \frac{1}{4}c^2,$$

und da $p < \sqrt{\frac{4}{3}c}$ ist, so ergiebt sich:

$$N > \frac{3}{2}c\sqrt{\frac{c}{48}}.$$

Diese Grenze ist gleich $\frac{3}{2}c$, wenn $c = 48$, und sie ist gröfser, sobald c gröfser ist als 48. Untersucht man ferner alle Fälle, in denen $c < 48$ ist, so begegnet man keiner Ausnahme von dem oben aufgestellten Satze. Demnach kann man allgemein behaupten, dafs, wenn $N < \frac{3}{2}c$ ist, die Zahl N nur einmal in einem quadratischen Teiler der Formel $t^2 + cu^2$, in welcher c eine Primzahl oder das Doppelte einer Primzahl ist, enthalten sein kann.

§ 14.

Über die Hülfsmittel zur Bestimmung einer Primzahl, welche gröfser ist als eine gegebene Zahl.

248.

Ist M eine Zahl, die zwei oder mehrere Male in der Formel $py^2 + 2qyz + rz^2$ enthalten ist, so dafs man

$$M = p\alpha^2 + 2q\alpha\beta + r\beta^2 = p\gamma^2 + 2q\gamma\delta + r\delta^2$$

hat, so wird, wenn man alles mit p multipliciert und wie gewöhnlich $pr - q^2 = c$ setzt:

$$(p\alpha + q\beta)^2 + c\beta^2 = (p\gamma + q\delta)^2 + c\delta^2.$$

Nehmen wir jetzt an, dafs c oder $\frac{1}{2}c$ eine Primzahl sei, oder dafs wenigstens, wenn eine oder die andere Zahl das Produkt zweier Faktoren ist, einer dieser Faktoren auch in p und q enthalten ist, so kann die vorstehende Gleichung nur stattfinden, wenn

$$p\alpha + q\beta \mp (p\gamma + q\delta)$$

durch c teilbar ist. Ist daher:

$$p\gamma + q\delta = \pm (p\alpha + q\beta - cx),$$

so erhält man, wenn man einsetzt und durch c dividiert, die Gleichung:

$$(a) \qquad \beta^2 + 2(p\alpha + q\beta)x - cx^2 = \delta^2.$$

Allemal, wo diese Gleichung möglich ist, d. h. allemal, wenn man einen von 0 verschiedenen Wert von x finden kann, für welchen die linke Seite ein vollständiges Quadrat wird, ergiebt sich, dafs die Zahl M oder die Hälfte derselben **keine** Primzahl ist.

249.

Wenn die Gleichung (a) nur für $x = 0$ möglich ist, so darf man noch nicht schliefsen, dafs die Zahl M oder die Hälfte derselben eine Primzahl sei. Wenn jedoch in eben diesem Falle der auf die Formel $t^2 + cu^2$ bezügliche quadratische Teiler $py^2 + 2qyz + rz^2$ der einzige seiner Art ist, so dafs eine in ihm enthaltene Zahl zu keinem andern quadratischen Teiler derselben Formel $t^2 + cu^2$ gehören kann, oder mit andern Worten, wenn der quadratische Teiler $py^2 + 2qyz + rz^2$ nur allein zu einer und derselben Gruppe von linearen Teilern gehört, wovon man in den Tafeln IV, V, VI und VII mannigfache Beispiele sieht, so behaupte ich, dafs man daraus

schliefsen kann, dafs die Zahl M oder die Hälfte derselben eine Primzahl ist, abgesehen von einer Ausnahme, die wir angeben werden.

1) Denn ist die Zahl M, welche in der Formel

$$py^2 + 2qyz + rz^2$$

enthalten ist, durch zwei Primzahlen teilbar, welche verschieden und Nichtteiler von c sind, so haben wir bereits gesehen (No. 246), dafs M auf zwei verschiedene Arten in der Formel $py^2 + 2qyz + rz^2$ enthalten ist, da diese die einzige ihrer Art ist. Mithin hat alsdann die Gleichung (a) mindestens zwei Lösungen.

2) Ist die Zahl M gleich einer geraden Potenz der Primzahl α, oder ist $M = \alpha^{2n}$, so gehört die Zahl M zu dem quadratischen Teiler $y^2 + cz^2$. Denn setzt man in diesem Teiler $y = \alpha^n$ und z gleich einer geraden Zahl, so erhält man dieselbe lineare Form $4cx + a$, welche der Zahl M zukommt. Nun setzt man aber voraus, dafs die linearen Formen, in denen M enthalten ist, nur einem einzigen quadratischen Teiler $py^2 + 2qyz + rz^2$ entsprechen; mithin ist dieser Teiler, in welchem M enthalten ist, nichts andres als $y^2 + cz^2$ oder der ihm äquivalente $y^2 + 2yz + (c + 1)z^2$. Nun bemerke ich, dafs die Zahl M, welche durch $f^2 + cg^2$, wo f und g zu einander prim sind, ausgedrückt ist, auch durch die einfache Formel γ^2 dargestellt werden kann, wenn man $y = \gamma = \alpha^n$, $z = 0$ setzt. Und obwohl dieser letztere Ausdruck nicht der Regel gemäfs ist, weil man y und z immer prim zu einander annehmen mufs, so bleibt es doch nicht minder richtig, dafs man $f^2 + cg^2 = \gamma^2$ setzen kann, und dafs somit die Gleichung (a) aufser der Lösung $x = 0$ noch eine andere besitzt, welche $\delta = 0$ ergiebt.

3) Ist die Zahl $M = \alpha^{2m+1}$, wo α eine Primzahl ist, so gehören, wie man leicht sieht, α und M zu demselben quadratischen Teiler. Denn ist $\alpha y^2 + 2\beta yz + \gamma z^2$ der quadratische Teiler, welcher α enthält, und setzt man $y = \alpha^m$ und z gleich einem Vielfachen von $2c$, so wird dieser Teiler von derselben linearen Form $4cx + a$, von welcher α^{2m+1} oder M ist. Nach Voraussetzung giebt es aber nur einen einzigen quadratischen Teiler, welcher der Gruppe von linearen Formen, in welcher M enthalten ist, entspricht. Mithin ist dieser Teiler $py^2 + 2qyz + rz^2$ identisch mit dem Teiler $\alpha y^2 + 2\beta yz + \gamma z^2$. Dieser enthält aber immer zwei Darstellungsweisen von M, eine, in welcher y und z prim zu einander sind, die andere, in der man $y = \alpha^m$ und $z = 0$ setzt. Mithin würde die Gleichung (a) diesen beiden Ausdrücken zufolge ebenfalls zwei Lösungen haben.

4) Ist $M = 2\alpha^{2m}$, so zeigt man in ähnlicher Weise, dafs die Zahl M zu dem quadratischen Teiler $2y^2 + 2yz + \left(\frac{c+1}{2}\right)z^2$ gehört, falls c ungerade, und zu dem Teiler $2y^2 + \frac{c}{2}z^2$, falls c gerade ist. In beiden Fällen läfst sich die Zahl M stets auf zwei Arten durch diesen Teiler darstellen; mithin besitzt die Gleichung (a) zwei Lösungen.

5) Ist die Zahl $M = 2\alpha^{2m+1}$, so zeigt man ebenfalls auf dieselbe Weise, dafs die Zahl M zu demselben quadratischen Teiler wie 2α gehört, und dafs somit dieser Teiler dargestellt werden kann durch $2\alpha y^2 + 2\beta yz + \gamma z^2$. Es giebt daher mindestens zwei Arten, der Gleichung $M = py^2 + 2qyz + rz^2$ zu genügen, und demgemäfs mindestens zwei Lösungen der Gleichung (a).

250.

Aus der Untersuchung aller dieser Fälle scheint hervorzugehen, dafs man, wenn die linke Seite der Gleichung (a) nur für $x = 0$ ein Quadrat werden kann, schliefsen könnte, dafs die Zahl M oder $\frac{1}{2}M$ eine Primzahl sei. Indessen mufs man den Fall ausnehmen, wo M einen Primfaktor α, der in c nicht enthalten ist, und mehrere andere $\beta, \gamma, \ldots$, die auch in c vorkommen, besitzt. Denn alsdann kann die Gleichung $\frac{x^2+c}{M} = e$ nur eine Lösung haben, und die Zahl M könnte nur auf eine Weise durch die Formel $py^2 + 2qyz + rz^2$ dargestellt werden. Wenn aber einerseits der quadratische Teiler

$$py^2 + 2qyz + rz^2,$$

welcher M enthält, der einzige seiner Art ist, wenn andererseits M mit c keinen Teiler gemeinsam hat und die Gröfse

$$\beta^2 + 2(p\alpha + q\beta)x - cx^2,$$

welche mit Hülfe des Wertes $M = p\alpha^2 + 2q\alpha\beta + r\beta^2$ gebildet ist, nur für $x = 0$ einem Quadrate gleich sein kann, so läfst sich mit Sicherheit aus diesen Bedingungen der Schlufs ziehen, dafs die Zahl M oder, falls sie gerade ist, die Hälfte derselben eine Primzahl ist.

251.

Nimmt man nun, nachdem dieses festgestellt ist, für α und β irgendwelche zu einander prime Zahlen, so kann man die folgenden Resultate, die wir aus mehreren andern analogen in unsern Tafeln

befindlichen ausgewählt haben, als ebenso viele Sätze betrachten. Sie geben verschiedene allgemeine Formeln, in denen jede in ihnen enthaltene Zahl eine Primzahl oder das Doppelte einer Primzahl ist, sobald die Bedingungs-Formel nur für $x = 0$ ein Quadrat sein kann, und zu gleicher Zeit sowohl M und c als auch α und β prim zu einander sind.

Bedingungs-Formel.	Formel der Primzahlen.
$\beta^2 + 2(\alpha + \beta)x - 13x^2$	$\alpha^2 + 2\alpha\beta + 14\beta^2$
$\beta^2 + 2(\alpha + \beta)x - 37x^2$	$\alpha^2 + 2\alpha\beta + 38\beta^2$
$\beta^2 + 6(\alpha + \beta)x - 57x^2$	$3\alpha^2 + 6\alpha\beta + 22\beta^2$
$\beta^2 + 6(\alpha + \beta)x - 93x^2$	$3\alpha^2 + 6\alpha\beta + 34\beta^2$
$\beta^2 + 6(5\alpha + \beta)x - 141x^2$	$15\alpha^2 + 6\alpha\beta + 10\beta^2$
$\beta^2 + 2(11\alpha + 7\beta)x - 193x^2$	$11\alpha^2 + 14\alpha\beta + 22\beta^2$
$\beta^2 + 2(2\alpha + \beta)x - 11x^2$	$\alpha^2 + \alpha\beta + 3\beta^2$
$\beta^2 + 2(2\alpha + \beta)x - 19x^2$	$\alpha^2 + \alpha\beta + 5\beta^2$
$\beta^2 + 2(2\alpha + \beta)x - 43x^2$	$\alpha^2 + \alpha\beta + 11\beta^2$
$\beta^2 + 2(2\alpha + \beta)x - 67x^2$	$\alpha^2 + \alpha\beta + 17\beta^2$
$\beta^2 + 6(2\alpha + \beta)x - 123x^2$	$3\alpha^2 + 3\alpha\beta + 11\beta^2$
$\beta^2 + 2(2\alpha + \beta)x - 163x^2$	$\alpha^2 + \alpha\beta + 41\beta^2$
$\beta^2 + 10(2\alpha + \beta)x - 235x^2$	$5\alpha^2 + 5\alpha\beta + 13\beta^2$
$\beta^2 + 2\alpha x - 10x^2$	$\alpha^2 + 10\beta^2$
$\beta^2 + 2\alpha x - 22x^2$	$\alpha^2 + 22\beta^2$
$\beta^2 + 2\alpha x - 58x^2$	$\alpha^2 + 58\beta^2$
$\beta^2 + 10\alpha x - 70x^2$	$5\alpha^2 + 14\beta^2$
$\beta^2 + 6\alpha x - 102x^2$	$3\alpha^2 + 34\beta^2$
$\beta^2 + 10\alpha x - 190x^2$	$5\alpha^2 + 38\beta^2$

252.

Um sich zu vergewissern, ob die Gröfse $\beta^2 + 2(p\alpha + q\beta)x - cx^2$ nur dann ein Quadrat sein kann, wenn $x = 0$ ist, mufs man versuchsweise für x alle ganzzahligen Werte setzen, welche zwischen den beiden Wurzeln der Gleichung $\beta^2 + 2(p\alpha + q\beta)x - cx^2 = 0$ liegen. Die Anzahl dieser Versuche ist also im Allgemeinen gleich $\frac{2}{c}\sqrt{pM}$,

wo M die Zahl $p\alpha^2 + 2q\alpha\beta + r\beta^2$ ist, deren Beschaffenheit man bestimmen will. Die vorteilhafteste Formel oder diejenige, welche die wenigsten Versuche erfordert, ist also die, in welcher unter sonst gleichen Umständen p am kleinsten und c am gröfsten ist.

Betrachtet man z. B. die Formel $\alpha^2 + \alpha\beta + 41\beta^2$, oder vielmehr, um sie mit der allgemeinen Formel $py^2 + 2qyz + rz^2$ in Übereinstimmung zu bringen, die Formel $2\alpha^2 + 2\alpha\beta + 82\beta^2$, so ist die Anzahl der Versuche, vermöge deren man sich Gewifsheit darüber verschafft, ob die Zahl $N = \alpha^2 + \alpha\beta + 41\beta^2$ eine Primzahl ist, gleich $\frac{4\sqrt{N}}{163}$ oder ungefähr $\frac{1}{41}\sqrt{N}$.

Die Formel $5\alpha^2 + 38\beta^2$, welche der Zahl $c = 190$ entspricht, ist noch vorteilhafter, wenigstens wenn man α ungerade nimmt. Denn setzt man $N = 5\alpha^2 + 38\beta^2$, so ist die Anzahl der Versuche gleich:

$$\frac{2\sqrt{5N}}{190} \text{ oder } \frac{2}{85}\sqrt{N} < \frac{4}{163}\sqrt{N}.$$

Nimmt man ferner in dieser zweiten Formel an, dafs auch β, ebenso wie α, ungerade sei, so kann die Gröfse $\beta^2 + 10\alpha x - 190x^2$ nicht von der Form $8n + 1$ und daher auch kein Quadrat werden, wofern man nicht x von der Form $4k$ oder $4k - \alpha$ annimmt. Da somit die Formen $4k + 2$, $4k + \alpha$ ausgeschlossen sind, so reduciert sich die Anzahl der Versuche auf $\frac{1}{85}\sqrt{N}$.

253.

Schliefslich kann man bemerken, dafs, je kleiner p ist, um so kleiner die Grenze von x wird. Nach allen diesen Betrachtungen dürfte die einfachste Art, eine Primzahl, welche gröfser als eine gegebene Grenze L ist, zu finden, die folgende sein:

Nachdem man $\alpha = 1$ gesetzt hat, nehme man für β eine ungerade Zahl, welche gröfser als $\sqrt{\frac{L}{38}}$ und nicht teilbar durch 5 ist. Dann ist die ungerade Zahl $5 + 38\beta^2$ gröfser als die gegebene Grenze L. Diese Zahl hat mit 190 keinen gemeinschaftlichen Teiler. Um also zu erfahren, ob N eine Primzahl ist, bleibt zu untersuchen, ob es einen von 0 verschiedenen Wert von x giebt, welcher die Gröfse $\beta^2 + 10x - 190x^2$ zu einem Quadrat macht. Die Werte von x, mit denen man den Versuch anzustellen hat, sind die sämtlichen, sowohl positiven wie negativen, Zahlen von der Form $4k$ oder $4k + 3$,

welche kleiner als $\frac{\beta}{\sqrt{190}}$ sind. Wenn für keine dieser Zahlen die in Rede stehende Gröfse gleich einem Quadrat ist, so folgt daraus, dafs die Zahl $5 + 38\beta^2$ eine Primzahl ist.

Es sei z. B. die Aufgabe gestellt, nach dieser Methode eine Primzahl zu finden, welche gröfser als 1000000 ist. Dazu nehme man β ungerade und $> \sqrt{\frac{1000000}{38}}$ an. Setzt man $\beta = 163$, so mufs man nachsehen, ob man der Gleichung

$$26569 + 10x - 190x^2 = y^2$$

genügen kann. Die Werte von x, mit denen der Versuch anzustellen ist, sind nur -1, 3, ± 4, -5, 7, ± 8, -9, 11, und da keine von diesen die linke Seite zu einem Quadrat macht, so folgt daraus, dafs die Zahl $5 + 38\beta^2 = 1009627$ eine Primzahl ist.

254.

Bei komplicierteren Beispielen würde man leicht die Anzahl der Versuche noch verringern können, wenn man auf die Reste achtet, welche die Quadrate bei der Division durch 3, durch 7, oder durch irgend eine andere Primzahl übrig lassen, und diejenigen Werte von x ausschliefst, welche diese Reste nicht geben können. Nimmt man z. B. $\beta = 3h$, so würde man finden, dafs x keine der vier Formen $9k + 3$, $9k + 4$, $9k + 6$, $9k + 7$ haben kann, wodurch sich die Anzahl der Versuche auf $\frac{5}{9}$ der Gesamtzahl reduciert. Wäre

$$\beta = 22h \pm 1,$$

so wären die auszuschliefsenden Werte $x = 11k + 1, 6, 8, 9, 10$, und die Anzahl der Versuche würde sich auf $\frac{6}{11}$ der Gesamtzahl reducieren. Durch Kombination dieser beiden Annahmen, d. h. wenn man $\beta = 66m \pm 21$ nimmt, würde sich die Anzahl der zu probierenden Werte von x auf $\frac{5}{9} \cdot \frac{6}{11}$ oder $\frac{10}{33}$ der Gesamtzahl, welche ungefähr gleich $\frac{1}{85}\sqrt{L}$ ist, reducieren und nur gleich $\frac{1}{280}\sqrt{L}$ werden.

Es sei z. B. $\beta = 681$. Um zu erfahren, ob die Zahl

$$5 + 38\beta^2 = 17622923$$

eine Primzahl ist, mufs man nachsehen, ob man der Gleichung



$$463761 + 10x - 190x^2 = y^2$$



genügen könne. Dem zufolge, was wir eben gefunden haben, reducieren sich die zu probierenden Werte von x auf die folgenden:

$$11,\ 27,\ 35,\ 36,\ 44,\ 47,\ -4,\ -8,\ -9,\ -17,\ -28,\ -37,\ -40,\ -44.$$

Der Wert 35 giebt nun: $y = 481$; mithin ist die in Rede stehende Zahl keine Primzahl.

Ist ferner $\beta = 747$, so erhält man den Ausdruck:

$$558009 + 10x - 190x^2,$$

in welchem man für x jede der folgenden Zahlen

$$11,\ 27,\ 35,\ 36,\ 44,\ 47,\ -4,\ -8,\ -9,\ -17,\ -28,\ -37,\ -40,\ -44,\ -52,\ -53$$

zu setzen hat. Da man findet, dafs für keine dieser Zahlen die Gröfse, um welche es sich handelt, eine Quadratzahl ist, so folgt daraus, dafs die Zahl 21204347 eine Primzahl ist.

255.

Nach diesen Prinzipien kann man in befriedigender Weise die Gründe dafür angeben, warum gewisse Formeln eine ziemlich grofse Reihe von Primzahlen einschliefsen (siehe Einleitung No. XX).

Z. B. findet man aus der Tafel (No. 251), dafs die Formel

$$\alpha^2 + \alpha + 41$$

gleich einer Primzahl sein mufs jedesmal, wenn die Gröfse

$$1 + (4\alpha + 2)x - 163x^2$$

nur für $x = 0$ eine Quadratzahl sein kann. Nun sieht man auf den ersten Blick, dafs diese Gröfse weder ein Quadrat noch auch eine positive Zahl sein kann, so lange $4\alpha + 2 < 163$ oder $\alpha < 40$ ist. Setzt man also der Reihe nach $\alpha = 0, 1, 2, 3, \ldots$ bis 39, so müssen alle Werte, welche sich dadurch für $\alpha^2 + \alpha + 41$ ergeben, Primzahlen sein.

Man sieht ebenso aus der Tafel in No. 251, dafs die Formel $\alpha^2 + 58$ eine Primzahl oder das Doppelte einer solchen darstellt, sobald $1 + 2\alpha x - 58x^2$ keine Quadratzahl sein kann (aufser für $x = 0$). Nun ist klar, dafs diese Gröfse kein Quadrat sein kann, so lange x unter 29 liegt. Mithin erkennt man von vornherein, dafs die 29 ersten, in der Formel $\alpha^2 + 58$ enthaltenen Zahlen Primzahlen oder das Doppelte von Primzahlen sein müssen.

Ebenso verhält es sich mit den 19 ersten in der Formel $5z^2 + 38$

enthaltenen Zahlen, da die Gröſse $1 + 10\alpha x - 190x^2$ kein Quadrat sein kann, so lange α unter 19 liegt.

Bemerkung. Die Aufgabe, eine Primzahl zu bestimmen, welche gröſser als eine gegebene Zahl ist, ist in diesem Paragraphen nicht vollständig gelöst. Wir haben nur verschiedene Formeln angegeben, bei denen es, wenn man eine in ihnen enthaltene Zahl, welche gröſser als die gegebene Grenze ist, willkürlich annimmt, schon sehr wahrscheinlich ist, daſs diese Zahl eine Primzahl ist. Um sich aber vollständige Gewiſsheit darüber zu verschaffen, muſs man Versuche anstellen, die um so langwieriger sind, je beträchtlicher die in Frage kommende Zahl ist. Überschreitet die Gröſse der Zahl gewisse Grenzen, so kann es vorteilhafter sein, die im folgenden Paragraphen angegebenen Methoden zu befolgen.

§ 15.

Anwendung der vorigen Sätze, um zu ermitteln, ob eine gegebene Zahl Primzahl ist oder nicht.

256.

Da die Primzahltafeln, welche man bis heute konstruiert hat, nicht sehr weit sich erstrecken, so wäre es für die weitere Vervollkommnung der Zahlentheorie wünschenswert, daſs man eine praktische Methode fände, mittelst deren man in Kürze entscheiden könnte, ob eine gegebene, die Grenzen der Tafeln überschreitende Zahl Primzahl ist oder nicht. So lange aber diese Methode noch nicht gefunden ist, wird es angebracht sein zu zeigen, welche Hülfsmittel zur Lösung dieses besonderen Problems man aus den bisher entwickelten Sätzen ableiten kann.

Wir haben bereits gesehen, daſs, wenn die gegebene Zahl A von der Form $a^n \pm 1$ ist, oder wenn sie auch nur ein Teiler dieser Formel ist, jede in A aufgehende Primzahl von der Form $nx + 1$ oder, falls n eine ungerade Zahl ist, von der Form $2nx + 1$ sein muſs. Denn wäre sie nicht von dieser Form, so würde sie in der kleineren Zahl $a^\nu \pm 1$, in welcher ν ein ungerader Teiler von n ist, aufgehen. Hat man also alle Zahlen $a^\nu \pm 1$, welche diese Bedingung erfüllen, untersucht, und geht keiner ihrer Primfaktoren in A auf, so ist man sicher, daſs die Teiler von A nur von der erwähnten Form $nx + 1$ oder $2nx + 1$ sein können, und wenn n ungerade ist, so müssen nicht nur die Teiler von A von der Form $2nx + 1$ sein, sondern

sie müssen auch eine der linearen Formen haben, welche den Teilern von $t^2 \pm au^2$ zukommen. Da diese Formen aus unsern Tafeln bekannt sind (wenigstens so lange a die Grenzen derselben nicht übersteigt), so kann man, durch Verbindung dieser beiden Bedingungen, die Anzahl der unterhalb $\sqrt{A}$ liegenden Primzahlen, mit denen man versuchsweise A dividieren mufs, bedeutend verringern. Von dieser Methode haben wir bereits in § 5 Beispiele gegeben; wir fügen noch die beiden folgenden hinzu.

257.

1) Betrachten wir die Zahl:

$$2^{25} - 1 = (2^5 - 1) \,.\, 1082401,$$

und stellen wir uns die Aufgabe, alle Teiler des Faktors $1082401 = A$ zu finden, so kann diese Zahl, da sie durch $2^5 - 1 = 31$ nicht teilbar ist, zu Teilern nur Zahlen von der Form $50x + 1$ haben. Da ferner die Zahl A ein Teiler der Formel $2^{26} - 2$ ist, und diese die Form $t^2 - 2u^2$ besitzt, so müssen die Teiler von A von der Form $8n + 1$ oder von der Form $8n + 7$ sein. Nun enthält die Form $50x + 1$ die vier andern:

$$200x + 1,\ 51,\ 101,\ 151.$$

Schliefst man daher die zweite und dritte, welche mit den Formen $8n + 1$ oder $8n + 7$ nicht vereinbar sind, aus, so bleiben für die Teiler von A nur die beiden Formen

$$200x + 1, \quad 200x + 151$$

übrig. Die in diesen Formen enthaltenen Zahlen, welche $\sqrt{A}$ nicht übersteigen, sind:

$$151,\ 201,\ 351,\ 401,\ 551,\ 601,\ 751,\ 801,\ 951,\ 1001.$$

Werden hiervon diejenigen ausgeschlossen, welche keine Primzahlen sind, so bleiben nur die vier Zahlen

$$151,\ 401,\ 601,\ 751$$

übrig, und mit diesen mufs man versuchen, A zu dividieren.

Die Division geht weder bei 151, noch bei 401, wohl aber bei 601 auf, und zwar erhält man 1801 zum Quotienten. Folglich ist A keine Primzahl. Was den Quotienten 1801 anlangt, so ist derselbe notwendigerweise eine Primzahl; denn wäre er es nicht, so müfste er sich durch eine Zahl dividieren lassen, die kleiner als $\sqrt{1801}$ wäre. Dies ist aber unmöglich, da die kleinste Zahl, welche in A aufgeht, 601 ist. Mithin ist einfach $A = 601 \cdot 1801$.

2) Betrachten wir die Zahl:

$$2^{27} - 1 = (2^9 - 1) \cdot 262657,$$

und stellen wir uns die Aufgabe, die Teiler der Zahl $A = 262657$ zu finden, so können wir uns leicht davon überzeugen, dafs diese Zahl durch keine von denen teilbar ist, welche in $2^3 - 1$ oder $2^9 - 1$ aufgehen. Mithin sind diese Teiler, falls es deren giebt, von der Form $54x + 1$. Da ferner A selbst ein Teiler von $2^{28} - 2$ ist, so sind die Teiler von A ebenfalls von der Form $t^2 - 2u^2$, und somit von einer der Formen $8n + 1$ und $8n + 7$. Kombiniert man also diese beiden Formen mit der Form $54x + 1$, so erhält man die beiden Formen:

$$216x + 1, \qquad 216x + 55,$$

und diese enthalten unterhalb der Grenze $\sqrt{A} = 512$, nur die fünf Zahlen:

$$55, 217, 271, 433, 487.$$

Scheidet man von diesen die zusammengesetzten Zahlen aus, so bleiben nur die drei Zahlen 271, 433, 487 übrig, und da keine von diesen drei Zahlen in 262657 aufgeht, so folgt daraus mit Sicherheit, dafs 262657 eine Primzahl ist.

258.

Überhaupt versuche man, wenn irgend eine Zahl A gegeben ist, diese Zahl oder eines ihrer Vielfachen auf die Form $t^2 + au^2$ zu bringen, in welcher die Zahl a so klein wie möglich ist und die Grenzen der Tafeln nicht übersteigt. Dazu mufs man die Quadratwurzel sowohl aus A wie aus einigen von seinen Vielfachen, $2A$, $3A$, $4A, \ldots$ ausziehen und es so einrichten, dafs der, positive oder negative, Rest von der Form au^2 wird, wo u^2 die gröfste Quadratzahl ist, durch welche sich dieser Rest teilen läfst.

Sobald man A oder allgemein kA auf die Form $t^2 \pm au^2$ gebracht hat, ist man sicher, dafs die Teiler von A unter den linearen Formen der Teiler von $t^2 \pm au^2$ enthalten sind. Und da durch diese linearen Formen die Hälfte der Primzahlen ausgeschlossen wird, so wird die Anzahl der Teiler, mit denen man die Division der Zahl A zu versuchen hat, so oftmal um die Hälfte verringert, als man für A oder kA verschiedene Formen $t^2 + au^2$ gefunden hat. Giebt es also m zwischen 1 und $\sqrt{A}$ enthaltene Primzahlen, und ist i die Anzahl der in Frage kommenden Formen $t^2 \pm au^2$, so hat

man nur noch mit $\left(\frac{1}{2}\right)^i \cdot m$ Primzahlen den Versuch zu machen, um sich Gewifsheit darüber zu verschaffen, ob A eine Primzahl ist oder nicht.

259.

Man kann endlich noch ein Hülfsmittel angeben, das sehr häufig zum Ziele führt. Es besteht darin, dafs man $\sqrt{A}$ oder $\sqrt{2A}$, $\sqrt{3A}, \ldots$ in einen Kettenbruch verwandelt. Ist nämlich allgemein $\frac{\sqrt{kA} + J}{D}$ ein aus der Entwicklung von $\sqrt{kA}$ hervorgehender vollständiger Quotient und $\frac{p}{q}$ der diesem Quotienten entsprechende Näherungsbruch, so ist (No. 30):

$$\pm D = p^2 - kAq^2 \quad \text{oder} \quad kAq^2 = p^2 \mp D.$$

Demnach sind die Teiler von A auch Teiler von $p^2 \mp D$ oder allgemein von $t^2 \mp Du^2$, nämlich von $t^2 + Du^2$, wenn der vollständige Quotient von gerader, und von $t^2 - Du^2$, wenn er von ungerader Ordnung ist.

Bei dieser Rechnung ist die Zahl D niemals gröfser als $2\sqrt{kA}$, sondern meistens bedeutend kleiner; mithin kann man auf diesem Wege ziemlich einfache Formeln $t^2 \pm Du^2$ kennen lernen, von denen die Faktoren von A Teiler sein müssen. Und wenn der Fall eintritt, dafs man zwei denselben Wert von D enthaltende Formeln $t^2 + Du^2$, $t^2 - Du^2$ findet, so folgt daraus, dafs A, welches in beiden aufgeht, auch in $t^2 + t'^2$ aufgeht, und dafs somit die Teiler von A selbst von der Form $y^2 + z^2$ und von der linearen Form $4x + 1$ sein müssen, wodurch die Rechnung sehr gekürzt wird.

260.

Diese Prinzipien wollen wir auf die Zahl $333667 = A$ anwenden. Durch Ausziehung der Quadratwurzel findet man zunächst $A = 577^2 + 82 \cdot 3^2$. Mithin ist A von der Form $t^2 + 82u^2$, und ihre Teiler müssen zu der Zahl derer gehören, welche dieser Formel zukommen. Um andere Formen zu finden, suchen wir Vielfache von A zu zerlegen. So erhalten wir z. B.

$$3A = 1001001 = (1001)^2 - 10(10)^2,$$

also eine Gröfse von der Form $t^2 - 10u^2$. Demnach müssen die Teiler von A eine von denjenigea Formen besitzen, welche den Teilern von $t^2 - 10u^2$ zukommen. Diese beiden Formen würden be-

reits die Primzahlen, die man als Teiler von A zu versuchen hat, und die kleiner als $\sqrt{A}$ oder 577 sein müssen, auf den vierten Teil reducieren. Da jedoch die Rechnung immer noch ziemlich lang werden würde, so suchen wir neue Formen mit Hülfe der Entwicklung in einen Kettenbruch. Diese Entwicklung liefert folgende vollständige Quotienten:

$$\frac{\sqrt{A}+0}{1},\quad \frac{\sqrt{A}+577}{738},\quad \frac{\sqrt{A}+161}{417},\quad \frac{\sqrt{A}+256}{643},\quad \frac{\sqrt{A}+387}{286},$$

$$\frac{\sqrt{A}+471}{391},\quad \frac{\sqrt{A}+311}{606},\quad \frac{\sqrt{A}+295}{407},\quad \frac{\sqrt{A}+519}{158},\quad \frac{\sqrt{A}+429}{947},$$

$$\frac{\sqrt{A}+518}{69},\quad \frac{\sqrt{A}+517}{962},\quad \frac{\sqrt{A}+445}{141},\quad \frac{\sqrt{A}+542}{288},\quad \text{u. s. w.}$$

Hieraus ersieht man, dafs die Teiler von A auch Teiler der Formeln

$$t^2 + 738u^2 \text{ oder } t^2 + 82u^2,\quad t^2 - 417u^2,\quad t^2 + 643u^2, \text{ u. s. w.}$$

sein müssen. Die einfachsten dieser Formeln sind $t^2 + 82u^2$, $t^2 - 69u^2$, und $t^2 + 2u^2$; denn auf diese letztere reduciert sich die Formel $t^2 + 288u^2$, welche unmittelbar durch das Glied $D = 288$ gegeben ist.

Fügt man zu diesen Formen die bereits gefundene $t^2 - 10u^2$ hinzu, so ist man im Stande, die Anzahl der noch übrigbleibenden Versuche bedeutend zu verringern. Da nun zunächst die Teiler von $t^2 + 2u^2$ von der Form $8n + 1$ oder $8n + 3$ und die von $t^2 - 10u^2$ von einer der Formen $40x + 1, 3, 9, 13, 27, 31, 37, 39$ sind, so bleiben, wenn man von diesen diejenigen Formen, welche nicht von der Form $8n + 1$ oder $8n + 3$ sind, ausscheidet, nur die Formen übrig:

$$40x + 1,\ 3,\ 9,\ 27.$$

Sucht man jetzt alle in diesen Formen enthaltenen Primzahlen bis zu 577, welches $\sqrt{A}$ ist, so findet man:

$$\dot{1},\ \dot{3},\ 4\dot{1},\ 4\dot{3},\ 6\dot{7},\ 83,\ 89,\ 107,\ 163,\ 227,\ 2\dot{4}1,\ 281,\ 2\dot{8}3,\ 34\dot{7},\ 401,$$
$$409,\ 44\dot{3},\ 44\dot{9},\ 467,\ 4\dot{8}1,\ 521,\ 5\dot{2}3,\ 547,\ 563,\ 569.$$

Scheidet man hiervon diejenigen aus, welche nicht Teiler von $t^2 - 69u^2$ sein können, und dies erkennt man leicht (Tafel III) mittelst der Formen $276x + a$, welche diesen Teilern zukommen, so bleiben die folgenden übrig:

$$1,\ 83,\ 8\dot{9},\ 107,\ 163,\ 2\dot{2}7,\ 2\dot{8}1,\ 401,\ 409,\ 467,\ 5\dot{2}1,\ 54\dot{7},\ 5\dot{6}3,\ 569.$$

Wirft man endlich von diesen letzteren diejenigen weg, welche nicht Teiler der Formel $t^2 + 82u^2$ sein können, oder welche nicht von der

diesen Teilern zukommenden Form $328x + a$ sind (Tafel VI), so hat man nur noch mit folgenden sieben Primzahlen den Versuch anzustellen:

$$83,\ 107,\ 163,\ 401,\ 409,\ 467,\ 569.$$

Nun geht aber keine von diesen Zahlen in 333667 auf; mithin ist 333667 sicher eine Primzahl.

Man würde die Anzahl der Versuche noch weit mehr verringert haben, wenn man bemerkt hätte, dafs, da

$$3A = 1001001 = 10^6 + 10^3 + 1 = \frac{10^9 - 1}{10^3 - 1}$$

ist, die Teiler von A auch in $10^9 - 1$ aufgehen und somit von der Form $18x + 1$ sein müssen. Wir haben indessen zeigen wollen, wie man verfahren müsse, wenn man nichts weiter von der Natur der zu untersuchenden Zahl weifs.

261.

Es sei ferner die Zahl $10091401 = A$ zu untersuchen. Nach dem allgemeinen Satze müfste man die Division durch sämtliche Primzahlen, welche kleiner als $\sqrt{A}$ d. h. kleiner als 3176 sind, versuchen. Um jedoch die Anzahl dieser Versuche zu verringern, suchen wir mit Hülfe der Kettenbruchentwicklung von $\sqrt{A}$ sogleich die verschiedenen Formeln $t^2 \pm Du^2$, von denen A ein Teiler sein mufs. Ist $\frac{\sqrt{A} + J}{D}$ der allgemeine Ausdruck des vollständigen Quotienten, so sind die durch diese Rechnung gelieferten Werte von D der Reihe nach:

$$\begin{array}{llll}
D = 1, & 4425 = 177 \cdot 5^2, & 1928 = 482 \cdot 2^2, & 1709, \\
2189, & 3033 = 337 \cdot 3^2, & 2872 = 718 \cdot 2^2, & 2511 = 31 \cdot 9^2, \\
3755, & 384 = 6 \cdot 8^2, & 5585, & 437, \\
3648 = 57 \cdot 8^2, & 2619, & 2495, & 183, \\
2019, & 720 = 5 \cdot 12^2, & 2963, & 152 = 38 \cdot 2^2, \\
2061 = 229 \cdot 3^2, & 365, & 480 = 30 \cdot 4^2, & 1119, \\
3415, & 2712 = 678 \cdot 2^2, & 2525 = 101 \cdot 5^2, & 3789 = 421 \cdot 3^2, \\
184 = 46 \cdot 2^2, & \text{u. s. w.} & &
\end{array}$$

Hieraus erhält man bereits mehrere ziemlich einfache Formeln, von denen A ein Teiler sein mufs. Diese Formeln sind:

$$t^2 + 31u^2,\quad t^2 + 6u^2,\quad t^2 - 57u^2,\quad t^2 + 5u^2,$$
$$t^2 + 38u^2,\quad t^2 - 30u^2,\quad t^2 - 46u^2.$$

Es ist jedoch zu beachten, dafs die Formel $t^2 - 30u^2$ nichts weiter aussagt, als die beiden vorhergehenden $t^2 + 6u^2$ und $t^2 + 5u^2$; denn ist eine Primzahl ein Teiler von $t^2 + 6u^2$ und von $t^2 + 5u^2$, so ist sie auch ein Teiler von $t^2 - 30u^2$. Ebenso ist die Formel $t^2 + 38u^2$ als in den beiden vorhergehenden $t^2 + 6u^2$ und $t^2 - 57u^2$ enthalten zu betrachten. Es bleiben daher von den sieben vorstehenden Formeln nur fünf von einander verschiedene übrig. Da eine jede von ihnen die Anzahl der Versuche auf die Hälfte zu reducieren vermag, so kann diese Anzahl durch Kombination derselben auf den zweiunddreifsigsten Teil verringert werden. Hierdurch reduciert sich die Anzahl der Versuche oder die Anzahl der Primzahlen, welche kleiner sind als $\sqrt{A}$, das ungefähr gleich 454 ist, auf 14 und die Rechnung wird praktisch durchführbar. Man hätte auch noch die Berechnung der Werte von D weiter fortsetzen können, wodurch man die neuen Formeln $t^2 - 55u^2$, $t^2 - 97u^2$, $t^2 + 3u^2$, von denen A ein Teiler sein mufs, erhalten hätte. Mit Berücksichtigung aller dieser Hülfsmittel erhält man die sämtlichen linearen Formen, welche den Teilern von A zukommen, in folgender Weise:

1) Die Teiler von $t^2 + 3u^2$ sind allgemein von der Form $6x + 1$, und diese enthält die vier Formen $24x + 1$, 7, 13, 19 in sich.

2) Von diesen vier Formen können nur zwei Teiler von $t^2 + 6u^2$ sein, nämlich $24x + 1$ und $24x + 7$.

3) Diese letzteren enthalten, mit Bezug auf die Vielfachen von 5 betrachtet, die acht Formen in sich: $120x + 1$, 7, 31, 49, 73, 79, 97, 103. Scheidet man von diesen diejenigen aus, welche nicht in $t^2 + 5u^2$ aufgehen können, so bleiben die vier Formen übrig:

$$120x + 1,\ 7,\ 49,\ 103.$$

Die in diesen Formen enthaltenen Primzahlen sind also gleichzeitig Teiler der drei Formen $t^2 + 3u^2$, $t^2 + 6u^2$, $t^2 + 5u^2$.

4) Werden die vorstehenden vier Formen mit Bezug auf die Vielfachen von 11 entwickelt, d. h. setzt man für x der Reihe nach $11x$, $11x + 1$, $11x + 2$ u. s. w., und wirft man die Vielfachen von 11 ab, so ergeben sich die folgenden vierzig Formen:

$$\begin{array}{rrrrrrrr} 1320x + 1, & 7, & 49, & 103, & 127, & 169, & 223, & 241, \\ 247, & 289, & 343, & 361, & 367, & 409, & 463, & 481, \\ 487, & 529, & 601, & 607, & 703, & 721, & 727, & 769, \\ 823, & 841, & 889, & 943, & 961, & 967, & 1009, & 1063, \\ 1081, & 1087, & 1129, & 1183, & 1201, & 1207, & 1249, & 1303. \end{array}$$

Von diesen Formen darf man nur diejenigen beibehalten, welche Teiler von $t^2 - 55u^2$ sein können. Zu diesem Zwecke entnehme man aus Tafel III die Formen $220x + a$, welche Teiler von $t^2 - 55u^2$ sind. Vergleicht man diese mit jenen, so bleiben nur die zwanzig Formen übrig:

$$\begin{aligned} 1320x + 1,\ 49,\ 103,\ 169,\ 223;\\ 247,\ 289,\ 361,\ 367,\ 463;\\ 487,\ 529,\ 727,\ 823,\ 841;\\ 889,\ 961,\ 1081,\ 1087,\ 1303. \end{aligned}$$

Nimmt man jetzt die in dieser Formel enthaltenen Zahlen, welche kleiner als 3176 sind, und schliefst man davon die zusammengesetzten Zahlen aus, so reducieren sie sich auf die folgenden:

103, 223, 367, 487, 727, 823, 1087, 1321, 1423, 1489,
1543, 1609, 1783, 2143, 2161, 2281, 2689, 3001, 3169.

Schliefst man ferner hiervon diejenigen Zahlen aus, welche nicht Teiler von $t^2 + 31u^2$ sein können, so bleiben die elf folgenden übrig:

103, 727, 1087, 1321, 1423, 1489, 1609, 1783, 2143, 2281, 3169.

Schliefst man endlich auch noch diejenigen aus, welche nicht Teiler von $t^2 + 38u^2$ sein können, so erhält man nur noch die sechs Zahlen:

727, 1087, 1423, 1489, 1783, 2281.

Die Bedingung, dafs diese Zahlen Teiler von $t^2 - 46u^2$ sein sollen, reduciert dieselben von neuem auf die drei Zahlen:

727, 1423, 2281.

Es ist unnütz, in der Reduktion dieser Zahlen noch weiter fortzufahren, ja man hätte sich auch der Mühe überheben können, soweit zu gehen. Nun findet man aber, dafs keine von diesen Zahlen in 10091401 aufgeht; mithin kann man mit Sicherheit schliefsen, dafs 10091401 eine Primzahl ist.

Euler ist zu demselben Resultate gelangt, indem er sich überzeugte, dafs 10091401 nur auf eine einzige Weise in die Summe zweier Quadrate zerlegt werden kann, was ein wesentliches Merkmal der Primzahlen von der Form $4n + 1$ ist. (Man sehe den IX. Bd. der Novi Comm. Petrop. Vergleiche auch die Abhandlungen der Berliner Akademie vom Jahre 1771).

Dritter Hauptteil.

Theorie der Zahlen, insofern sie sich in drei Quadrate zerlegen lassen.

§ 1.

Definition der trinären Form; Zahlen und quadratische Teiler, welche diese Form besitzen oder nicht besitzen können.

262.

Die Zahlen, welche sich in drei Quadrate zerlegen lassen, bilden verschiedene sehr umfangreiche Klassen, welche eine sehr grofse Zahl von schönen Eigenschaften besitzen und in dieser Beziehung wert sind, dafs sich die Aufmerksamkeit der Analysten ihnen zuwende. Zur Abkürzung nennen wir **trinäre Form** einer Zahl jede Art, diese Zahl als **Summe von drei Quadraten** darzustellen. Da z. B. 59 durch $25 + 25 + 9$ und durch $49 + 9 + 1$ dargestellt werden kann, so ist jeder dieser Ausdrücke eine trinäre Form oder ein trinärer Wert von 59.

Eine trinäre Form besteht im Allgemeinen aus drei Quadraten. Sie kann jedoch auch blofs aus zweien oder selbst aus einem einzigen Quadrate bestehen, da in diesen Fällen 0 als ergänzendes Quadrat betrachtet wird. So besitzt z. B. 26 die beiden in gleicher Weise trinären Formen $25 + 1$ und $16 + 9 + 1$.

263.

Wenn eine Zahl durch eine Quadratzahl teilbar ist, so sind die dieser Zahl eigentümlichen trinären Formen diejenigen, in welchen die drei Glieder nicht durch eine und dieselbe Quadratzahl teilbar sind. Diejenigen dagegen, deren drei Glieder einen gemeinsamen Teiler haben, sind gewissermafsen dieser Zahl fremd und

müssen als **uneigentliche** trinäre Formen betrachtet werden. So besitzt z. B. 189 drei **eigentliche** trinäre Formen, nämlich:

$$13^2 + 4^2 + 2^2$$
$$10^2 + 8^2 + 5^2$$
$$11^2 + 8^2 + 2^2,$$

und eine uneigentliche trinäre Form, nämlich $12^2 + 6^2 + 3^2$. Da nämlich die drei Glieder dieser letzteren durch 3^2 teilbar sind, so ist dieser Wert nichts anderes als eine trinäre Form von 21, nämlich $4^2 + 2^2 + 1^2$, deren sämtliche Glieder mit 3^2 multipliciert sind.

Die uneigentlichen trinären Formen einer Zahl $\alpha^2 c$ entstehen aus den eigentlichen trinären Formen der Zahl c dadurch, daſs man die Glieder dieser letzteren mit α^2 multipliciert. Giebt es mehrere verschiedene Quadratzahlen, welche in einer gegebenen Zahl aufgehen, so giebt es auch mehrere Arten, um uneigentliche trinäre Formen zu bestimmen. Aus diesem Grunde werden wir in allem Folgenden stets nur die eigentlichen trinären Formen der Zahlen betrachten; wir werden dieselben einfach trinäre Formen nennen und von den uneigentlichen trinären Formen ganz absehen.

264.

Eine eigentliche trinäre Form kann auch nur aus zwei Quadraten bestehen, vorausgesetzt, daſs dieselben keinen gemeinsamen Teiler besitzen; denn fügt man das ergänzende Quadrat 0^2 hinzu, so sind die drei Glieder nicht durch eine und dieselbe Zahl teilbar. So ist z. B. $25 + 16$ ebenso gut eine trinäre Form von 41, wie $36 + 4 + 1$.

Dagegen kann ein einzelnes Quadrat auſser 1 keine trinäre Form sein, da die drei Glieder von $m^2 + 0^2 + 0^2$ durch m^2 teilbar sind.

265.

Keine Zahl von der Form $8n + 7$ kann eine trinäre Form haben.

Denn da jedes gerade Quadrat von der Form $4m$ und jedes ungerade Quadrat von der Form $8m + 1$ ist, so kann die Summe von drei Quadraten, falls sie ungerade ist, nur von einer der Formen

$$4m + 4m' \qquad + 8m'' + 1 = 4k + 1$$
$$8m + 1 + 8m' + 1 + 8m'' + 1 = 8k + 3$$

sein, und diese enthalten nicht die Form $8n + 7$.

Ebenso kann keine Zahl von der Form $4n$ eine eigentliche trinäre Form besitzen.

Denn da nicht alle drei Quadrate gerade sein können, weil der Fall, wo sie einen gemeinschaftlichen Teiler haben, ausgeschlossen ist, so kann die aus ihnen entstehende Summe nur von der Form

$$4m + 8m' + 1 + 8m'' + 1 = 4k + 2$$

sein, und diese ist nicht teilbar durch 4.

266.

Nachdem auf diese Weise die Formen $8n + 7$ und $4n$ ausgeschlossen sind, bleiben nur die drei allgemeinen Formen $4n + 1$, $4n + 2$ und $8n + 3$ übrig. In diesen müssen alle Zahlen, welche trinäre Formen haben können, enthalten sein. Die Theorie, die wir entwickeln wollen, zeigt nun aber, dafs jede in diesen Formen enthaltene Zahl auch wirklich auf eine oder mehrere Arten in drei Quadrate, welche sich nicht durch denselben Faktor teilen lassen, zerlegbar ist.

267.

Wenn die Zahl c zu einer der Formen $4n + 1$, $4n + 2$, $8n + 3$ gehört, so wird in gleicher Weise die Formel $t^2 + cu^2$ stets in den beiden ersten Fällen wenigstens einen, in dem dritten Falle einen zweifachen quadratischen Teiler von der Beschaffenheit besitzen, dafs man denselben in unbestimmter Weise, also ohne dafs man den darin auftretenden unbestimmten Gröfsen y und z besondere Werte beilegt, in drei Quadrate zerlegen kann. So zerlegt sich z. B. der zur Formel $t^2 + 65u^2$ gehörige quadratische Teiler $9y^2 + 8yz + 9z^2$ in drei Quadrate, nämlich: $(2y - z)^2 + (2y + 2z)^2 + (y + 2z)^2$.

Da diese Zerlegung ein eigentümliches Kennzeichen für diese Art von Teilern liefert, so werden wir diejenigen, welche dasselbe besitzen, **trinäre quadratische Teiler** oder einfach **trinäre Teiler** nennen. Dieselben müssen jedoch aufserdem noch einer Bedingung genügen, die wir später angeben werden; denn sonst würde die trinäre Form eine uneigentliche sein und zu denen gehören, von denen wir absehen.

268.

Wir bemerken, dafs es gewisse Klassen von quadratischen Teilern giebt, die **niemals** von trinärer Form sein können.

1) Ist c von der Form $4n + 1$, so sind die quadratischen Teiler der Formel $t^2 + cu^2$ von zweierlei Art; die eine enthält die Teiler

von der Form $4n + 1$, die andere enthält die Teiler von der Form $4n + 3$. Diese schliefsen zugleich die Zahlen von der Form $8n + 3$ und $8n + 7$ ein. Da nun keine Zahl von der Form $8n + 7$ eine trinäre Form haben kann, so folgt daraus, dafs auch kein quadratischer Teiler von der Form $4n + 3$ eine trinäre Form besitzen kann.

2) Ist c von der Form $8n + 7$, so giebt es absolut keinen quadratischen Teiler der Formel $t^2 + cu^2$, welcher von trinärer Form wäre. Der Grund hiervon ist, dafs jeder quadratische Teiler die Zahlen $4n + 1$ und $4n + 3$ ohne Unterschied enthält; derselbe enthält also auch die Zahlen von der Form $8n + 7$, von denen keine von trinärer Form ist.

3) Ist c von der Form $8n + 3$, so kann es aus demselben Grunde keinen ungeraden quadratischen Teiler geben, der von trinärer Form wäre. Jedoch kann es vorkommen, — und es kommt, wie bereits erwähnt, in allen Fällen wirklich vor —, dafs wenigstens einer von den ungeraden quadratischen Teilern, wenn man ihn verdoppelt, von trinärer Form ist. So stellt z. B. $y^2 + yz + 5z^2$ jeden ungeraden quadratischen Teiler der Formel $t^2 + 19u^2$ dar. Dieser quadratische Teiler ist nicht von trinärer Form; wohl aber ist das Doppelte desselben $2y^2 + 2yz + 10z^2$ von dieser Form, da dieses sich in die folgenden drei Quadrate auflöst: $y^2 + (3z)^2 + (y + z)^2$.

§ 2.

Gegenseitiges Entsprechen der trinären Formen der Zahl c und der trinären Teiler der Formel $t^2 + cu^2$.

269.

Ist ein quadratischer Teiler der Formel $t^2 + cu^2$ in drei Quadrate zerlegbar, wie folgt:

$$(my + nz)^2 + (m'y + n'z)^2 + (m''y + n''z)^2,$$

so behaupte ich, dafs aus dieser trinären Form des Teilers eine entsprechende trinäre Form der Zahl c sich ergiebt, und zwar ist diese:

$$c = (mn' - m'n)^2 + (m'n'' - m''n')^2 + (m''n - mn'')^2.$$

Stellt man nämlich den quadratischen Teiler, um den es sich handelt, durch die gewöhnliche Formel

$$py^2 + 2qyz + rz^2$$

dar, so erhält man:



$$p = m^2 + m'^2 + m''^2$$
$$q = mn + m'n' + m''n''$$
$$r = n^2 + n'^2 + n''^2.$$

Werden nun diese Werte in die Gleichung $c = pr - q^2$ eingesetzt, so folgt daraus:

$$c = (mn' - m'n)^2 + (m'n'' - m''n')^2 + (m''n - mn'')^2.$$

Es giebt daher stets eine bestimmte trinäre Form von c, welche einer bestimmten trinären Form des quadratischen Teilers

$$py^2 + 2qyz + rz^2$$

entspricht.

270.

Bemerkung 1. Ist c von der Form $8k + 3$, so betrachte man an Stelle des quadratischen Teilers mit ungeraden Koefficienten, welcher niemals von trinärer Form sein kann, das Doppelte desselben $2py^2 + 2qyz + 2rz^2$, wobei $4pr - q^2 = c$ ist. Wenn daher dieser verdoppelte Teiler in drei Quadrate zerlegbar ist, so giebt es immer einen entsprechenden Wert von c, der ebenfalls durch die Summe dreier bestimmten Quadrate ausgedrückt wird, d. h. mit andern Worten, jede trinäre Form eines quadratischen Teilers von der Form $4n + 2$ liefert eine entsprechende Form der Zahl c. Letztere ist immer aus drei ungeraden Quadraten zusammengesetzt, denn nur diese Annahme liefert eine Summe von der Form $8k + 3$.

Bemerkung 2. Die Zerlegung eines quadratischen Teilers oder des Doppelten desselben in drei Quadrate ist nicht möglich, wenn $c = 8k + 7$. Denn wenn diese Zerlegung möglich wäre, so würde aus dem vorstehenden Satze folgen, dafs c die Summe dreier Quadrate sei, was jedoch für keine Zahl von der Form $8k + 7$ der Fall ist.

Bemerkung 3. Die im Allgemeinen für den Wert von c gefundenen drei Quadrate reducieren sich auf zwei oder auch auf ein einziges in den folgenden, leicht zu erkennenden Fällen.

1) Ist $(m''n' - m'n'')^2 = 0$ oder $\frac{m''}{n''} = \frac{m'}{n'}$, so mufs das Quadrat $(m''y + n''z)^2$ zu dem Quadrat $(m'y + n'z)^2$ ein konstantes Verhältnis haben, und alsdann besitzt der gegebene quadratische Teiler Δ die Form:

$$\Delta = (my + nz)^2 + \alpha^2(m'y + n'z)^2 + \beta^2(m'y + n'z)^2.$$

Hieraus ergiebt sich der entsprechende trinäre Wert:

$$c = \alpha^2(m'n - mn')^2 + \beta^2(m'n - mn')^2,$$



welcher nur aus zwei Quadraten besteht. Überdies besitzen diese beiden Quadrate einen gemeinschaftlichen Teiler; es ist daher die trinäre Form von c eine uneigentliche, wofern nicht $mn' - m'n = \pm 1$ ist. Setzt man aber alsdann $my + nz = y'$ und $m'y + n'z = z'$, wodurch die Allgemeinheit der Werte von y und z nicht beschränkt wird (No. 53), so geht Δ über in $y'^2 + (\alpha^2 + \beta^2)z'^2$ oder $y'^2 + cz'^2$. Hat daher c keinen quadratischen Faktor, und ist c nicht gleich $\alpha^2 + \beta^2$, so kann der eben betrachtete Fall nicht eintreten; vielmehr mufs jeder trinäre Teiler der Formel $t^2 + cu^2$ einen trinären Wert von c geben, der aus drei Quadraten besteht, von denen keins gleich 0 ist.

2) Wenn die drei Quadrate, welche den aus dem Teiler Δ abgeleiteten Wert von c bilden, sich auf ein einziges reducieren, d. h. wenn $m''n' - m'n'' = 0$ und $m''n - mn'' = 0$ ist, so ergiebt sich $m'' = 0$, $n'' = 0$. Alsdann ist also der in Rede stehende quadratische Teiler einfach $(my + nz)^2 + (m'y + n'z)^2$, und der entsprechende Wert von c ist $c = (mn' - m'n)^2$. Dieser gehört aber nur dann zu den eigentlichen trinären Formen, wenn $c = 1$ ist.

271.

Wir betrachten von nun an als trinäre Form eines quadratischen Teilers **nur diejenige**, aus welcher sich eine eigentliche trinäre Form der Zahl c ergiebt. Wenn daher die drei Zahlen $mn' - m'n$, $m'n'' - m''n'$, $m''n - mn''$ durch einen und denselben Faktor teilbar wären, so würde der Ausdruck

$$\Delta = (my + nz)^2 + (m'y + n'z)^2 + (m''y + n''z)^2$$

eine uneigentliche trinäre Form sein, und diese müfste ausgeschlossen werden, da ihr nicht die Eigenschaften zukommen, die wir von den trinären Teilern beweisen werden. Diese Bedingung, die wir hier den trinären Teilern auferlegt haben, ist die bereits in No. 267 angekündigte.

Obgleich demnach der Teiler $5y^2 + 2yz + 38z^2$ der Formel $t^2 + 189u^2$ die folgenden vier trinären Formen annehmen kann:

$$(2y + 3z)^2 + (y - 5z)^2 + 4z^2$$
$$(2y + 2z)^2 + (y - 3z)^2 + 25z^2$$
$$(2y + z)^2 + (y - z)^2 + 36z^2$$
$$(2y - 2z)^2 + (y + 5z)^2 + 9z^2,$$

so betrachtet man doch, weil die beiden letzten der uneigentlichen trinären Form $c = 12^2 + 6^2 + 3^2$ entsprechen, als trinäre Formen

von Δ nur die beiden ersten, welche eigentlichen trinären Formen von c entsprechen, nämlich:

$$c = 13^2 + 4^2 + 2^2$$
$$c = 10^2 + 8^2 + 5^2.$$

Ebenso darf der Teiler $13y^2 + 8yz + 13z^2$ der Formel $t^2 + 153u^2$, da er sich nur auf folgende Weise

$$(2y + 2z)^2 + 9y^2 + 9z^2$$

in drei Quadrate zerlegen läſst, und diese einem uneigentlichen trinären Werte von c entspricht, nämlich:

$$c = 9^2 + 6^2 + 6^2,$$

nicht zu den trinären Teilern der Formel $t^2 + 153u^2$ gerechnet werden.

272.

So wie man mit Hülfe eines trinären Teilers der Formel $t^2 + cu^2$ einen entsprechenden trinären Wert von c finden kann, so ist es auch **umgekehrt**, wenn der trinäre Wert von c gegeben ist, möglich, einen diesem Werte entsprechenden trinären Teiler zu finden. Diese Aufgabe, mit der wir uns jetzt beschäftigen wollen, erfordert eine ziemlich ausgedehnte Untersuchung.

Die gegebene trinäre Form sei:

$$c = F^2 + G^2 + H^2.$$

Die drei Zahlen F, G, H können nicht alle drei, wohl aber zu je zweien einen gemeinschaftlichen Teiler haben. Nennen wir λ den gemeinschaftlichen Teiler von G und H, μ den von H und F und ν den von F und G, so können wir c die folgende Form geben:

$$c = f^2\mu^2\nu^2 + g^2\nu^2\lambda^2 + h^2\lambda^2\mu^2,$$

und müssen überdies voraussetzen, daſs es weder zwischen $f\mu$ und $g\lambda$, noch zwischen $g\nu$ und $h\mu$, noch zwischen $h\lambda$ und $f\nu$ einen gemeinsamen Teiler giebt.

Ist Δ der diesem Werte von c entsprechende trinäre Teiler, und nehmen wir an, daſs

$$\Delta = (my + nz)^2 + (m'y + n'z)^2 + (m''y + n''z)^2$$

sei, so muſs der gegebene Wert von c mit demjenigen identisch sein, welchen man aus diesem Teiler erhält, und welcher lautet:

$$c = (mn' - m'n)^2 + (m'n'' - m''n')^2 + (m''n - mn'')^2.$$

Da die Koefficienten $m, n, m', \ldots$ noch unbestimmt sind, so kann die Vergleichung der beiden Werte in beliebiger Ordnung vorgenommen



werden. Ferner kann man die Zeichen von f, g, h beliebig ändern, so dafs man setzen kann:

$$mn' - m'n = h\lambda\mu$$
$$m'n'' - m''n' = f\mu\nu$$
$$m''n - mn'' = g\nu\lambda.$$

Aus diesen drei Gleichungen leitet man die beiden folgenden, welche linear sind, her:

$$f\mu\nu \cdot m + g\nu\lambda \cdot m' + h\lambda\mu \cdot m'' = 0$$
$$f\mu\nu \cdot n + g\nu\lambda \cdot n' + h\lambda\mu \cdot n'' = 0,$$

oder, was dasselbe ist:

$$f \cdot \frac{m}{\lambda} + g \cdot \frac{m'}{\mu} + h \cdot \frac{m''}{\nu} = 0$$
$$f \cdot \frac{n}{\lambda} + g \cdot \frac{n'}{\mu} + h \cdot \frac{n''}{\nu} = 0.$$

Wie wir aber bereits bemerkt haben, giebt es weder zwischen f und λ, noch zwischen g und μ, noch zwischen h und ν einen gemeinschaftlichen Teiler. Mithin sind die sechs Gröfsen

$$\frac{m}{\lambda}, \quad \frac{m'}{\mu}, \quad \frac{m''}{\nu}, \quad \frac{n}{\lambda}, \quad \frac{n'}{\mu}, \quad \frac{n''}{\nu}$$

ganze Zahlen. Nennt man diese ganzen Zahlen entsprechend a, a', a'', b, b', b'', so erhält man die drei Gleichungen:

$$ab' - a'b = h$$
$$(a) \qquad fa + ga' + ha'' = 0$$
$$fb + gb' + hb'' = 0,$$

und der Teiler Δ geht über in:

$$\Delta = \lambda^2(ay + bz)^2 + \mu^2(a'y + b'z)^2 + \nu^2(a''y + b''z)^2.$$

Hieraus erkennt man, dafs die drei Quadrate, aus denen Δ besteht, resp. teilbar sind durch die Quadrate λ^2, μ^2, ν^2, welche zu je zweien die Glieder des gegebenen trinären Wertes

$$c = f^2\mu^2\nu^2 + g^2\nu^2\lambda^2 + h^2\lambda^2\mu^2$$

teilen.

273.

Ohne auf die Einzelheiten der Auflösung der Gleichungen (a) einzugehen, sieht man jetzt, dafs, wenn man

$$ay + bz = x, \qquad a'y + b'z = x', \qquad a''y + b''z = x''$$

setzt, man erhält:

$$(a') \qquad \Delta = \lambda^2x^2 + \mu^2x'^2 + \nu^2x''^2,$$

wobei die drei unbestimmten Gröfsen x, x', x'' der Gleichung

$$(a'') \qquad 0 = fx + gx' + hx''$$

genügen müssen. Mittelst dieser letzten Gleichung kann man stets die drei unbestimmten Gröfsen x, x', x'' nur auf zwei y und z reducieren; alsdann nimmt der Teiler $\lambda^2 x^2 + \mu^2 x'^2 + \nu^2 x''^2$ die gewöhnliche Form $py^2 + 2qyz + rz^2$ an, in der $pr - q^2 = c$ ist. Dieser Teiler ist derjenige, welchem der gegebene trinäre Wert von c entspricht.

Sucht man z. B. den trinären Teiler von $t^2 + 1045u^2$, welcher dem trinären Werte $1045 = 30^2 + 9^2 + 8^2$ entspricht, so vergleiche man diesen Wert Glied für Glied mit der Formel

$$f^2\mu^2\nu^2 + g^2\nu^2\lambda^2 + h^2\lambda^2\mu^2.$$

Dies giebt zunächst die gemeinsamen Teiler $\lambda = 1$, $\mu = 2$, $\nu = 3$ und sodann $f = 5$, $g = 3$, $h = 4$. Man erhält daher:

$$\Delta = x^2 + 4x'^2 + 9x''^2$$

und:

$$5x + 3x' + 4x'' = 0.$$

Diese letztere Gleichung wird befriedigt, wenn man

$$x' = x - 4z \quad \text{und} \quad x'' = 3z - 2x$$

setzt. Dadurch geht der Teiler Δ über in:

$$\Delta = x^2 + (2x - 8z)^2 + (9z - 6x)^2$$
$$= 41x^2 - 140xz + 145z^2.$$

Setzt man sodann $x = y + 2z$, so erhält man seinen einfachsten Ausdruck:

$$\Delta = 41y^2 + 24yz + 29z^2 = (y + 2z)^2 + (2y - 4z)^2 + (6y + 3z)^2$$

und der entsprechende Wert von c ist:

$$c = 8^2 + 9^2 + 30^2.$$

274.

Die Form der Gleichungen (a'), (a'') läfst erkennen, dafs man irgend zwei der Gröfsen f, g, h mit einander vertauschen kann, wofern man eine analoge Vertauschung bei zweien der Gröfsen λ, μ, ν vornimmt. Der quadratische Teiler Δ bleibt dabei stets derselbe. Es kann somit nur einen einzigen quadratischen Teiler der Formel $t^2 + cu^2$ geben, welcher dem gegebenen trinären Werte von c entspricht. Da jedoch diese Eigenschaft sehr beachtenswert



ist, so dürfte es nicht unnützlich sein, wenn wir uns davon durch eine andere Betrachtung überzeugen.

Auf welche Weise man auch der Gleichung $0 = fx + gx' + hx''$ genügen möge, indem man die drei Veränderlichen x, x', x'' auf zwei andere y und z reduciert, es mufs immer der transformierte Teiler $\Delta = py^2 + 2qyz + rz^2$ dieselben Zahlen enthalten, welche mit Berücksichtigung der Bedingung $fx + gx' + hx'' = 0$ in dem nicht transformierten Teiler $\Delta = \lambda^2 x^2 + \mu^2 x'^2 + \nu^2 x''^2$ enthalten sind. Sind demnach k und k' die beiden kleinsten, in dem Teiler

$$\lambda^2 x^2 + \mu^2 x'^2 + \nu^2 x''^2$$

enthaltenen Zahlen, so müssen diese nämlichen beiden Zahlen sich in dem transformierten Teiler wiederfinden. Wenn nun, wie man annehmen darf, dieser Teiler auf die einfachste Form gebracht ist, so sind p und r die beiden kleinsten in ihm enthaltenen Zahlen (No. 56). Mithin müssen p und r gleich k und k' sein, so dafs der reducierte Teiler ist: $ky^2 + 2qyz + k'z^2$. Ferner mufs stets $kk' - q^2 = c$ sein, so dafs q bestimmt ist. Daher kann es nur einen quadratischen Teiler geben, welcher mit Berücksichtigung der Bedingung

$$fx + gx' + hx'' = 0$$

durch Transformation von $\lambda^2 x^2 + \mu^2 x'^2 + \nu^2 x''^2$ entsteht.

Zugleich bemerken wir, dafs, wenn man $x'' = 0$ setzt, die Gleichung $fx + gx' = 0$ ergiebt: $x' = f$, $x = -g$ und $\Delta = \lambda^2 g^2 + \mu^2 f^2$. Ebenso giebt die Annahme $x' = 0$: $\Delta = \lambda^2 h^2 + \mu^2 f^2$ und die Annahme $x = 0$: $\Delta = \mu^2 h^2 + \nu^2 g^2$. Diese drei Zahlen müssen demnach in dem transformierten Teiler $\Delta = py^2 + 2qyz + rz^2$ enthalten sein.

275.

Wie wir soeben bewiesen haben, kann ein und derselbe Wert von c nur einem **einzigen** quadratischen **Teiler** entsprechen; es ist jedoch möglich, dafs er **zwei** trinären **Formen** dieses Teilers entspricht. So kann der Teiler $5y^2 + 4yz + 5z^2$, welcher zur Formel $t^2 + 21u^2$ gehört, auf die beiden trinären Formen gebracht werden:

$$(2y + z)^2 + y^2 + 4z^2$$
$$(y + 2z)^2 + z^2 + 4y^2,$$

und diese beiden Formen entsprechen einem und demselben Werte von c, nämlich $c = 16 + 4 + 1$. Man mufs daher notwendig von vornherein bestimmen, welches die verschiedenen Fälle sind, in

denen **verschiedene** trinäre Formen eines quadratischen Teilers **denselben** trinären Wert von c ergeben.

Da zwei beliebige der drei Zahlen f, g, h prim zu einander sind, so kann man stets zwei andere ζ und ϑ finden, welche der Gleichung

$$f = g\zeta + h\vartheta$$

genügen. Setzt man diesen Wert in die Gleichung $0 = fx + gx' + hx''$ ein, so erhält man:

$$g(x' + \zeta x) + h(x'' + \vartheta x) = 0,$$

und hieraus ist ersichtlich, dafs, wenn man $x' + \zeta x = -hu$ setzt, $x'' + \vartheta x = gu$ wird. Alsdann geht der Teiler Δ über in:

$$\Delta = \lambda^2 x^2 + \mu^2(hu + \zeta x)^2 + \nu^2(gu - \vartheta x)^2,$$

und dieser reduciert sich auf die gewöhnliche Form

$$Au^2 + 2Bux + Cx^2,$$

wenn man

$$A = \mu^2 h^2 + \nu^2 g^2$$
$$B = \mu^2 \zeta h - \nu^2 \vartheta g$$
$$C = \lambda^2 + \mu^2 \zeta^2 + \nu^2 \vartheta^2$$

setzt.

276.

Ist jetzt $py^2 + 2qyz + rz^2$ der einfachste Ausdruck dieses Teilers und ist eine der trinären Formen, welche dem gegebenen Werte von c entsprechen, die folgende:

$$\Delta = \lambda^2(ay + bz)^2 + \mu^2(a'y + b'z)^2 + \nu^2(a''y + b''z)^2,$$

so mufs man haben:

$$p = \lambda^2 a^2 + \mu^2 a'^2 + \nu^2 a''^2$$
$$q = \lambda^2 ab + \mu^2 a'b' + \nu^2 a''b''$$
$$r = \lambda^2 b^2 + \mu^2 b'^2 + \nu^2 b''^2,$$

und damit die angenommene trinäre Form dem gegebenen Werte von c entspreche, mufs man überdies den Gleichungen genügen:

$$ab' - a'b = h$$
$$fa + ga' + ha'' = 0$$
$$fb + gb' + hb'' = 0.$$

Ist wie oben $f = g\zeta + h\vartheta$, so kann man die beiden letzten Gleichungen durch Einführung zweier unbestimmten Gröfsen α und β in folgender Weise auflösen:

$$a' = -\zeta a + h\alpha, \qquad b' = -\zeta b + h\beta$$
$$a'' = -\vartheta a - g\alpha, \qquad b'' = -\vartheta b - g\beta,$$

und die Gleichung $ab' - a'b = h$ geht über in:

$$a\beta - \alpha b = 1.$$

Setzt man jetzt die Werte von $a', a'', \ldots$ in die Ausdrücke der Koefficienten p, q, r ein, so erhält man:

$$p = A\alpha^2 - 2Ba\alpha + Ca^2$$
$$q = A\alpha\beta - B(a\beta + \alpha b) + Cab$$
$$r = A\beta^2 - 2Bb\beta + Cb^2.$$

Da wir aber bereits die Bedingung $pr - q^2 = c$ ausgedrückt haben, so können wir von der zweiten Gleichung absehen und nur die beiden andern betrachten:

$$p = A\alpha^2 - 2Ba\alpha + Ca^2$$
$$r = A\beta^2 - 2Bb\beta + Cb^2.$$

Diese Werte stimmen mit denjenigen überein, welche man erhalten würde, wenn man den Teiler $\Delta = Au^2 + 2Bux + Cx^2$ auf die einfachste Form bringt. Denn setzt man:

$$u = -\alpha y - \beta z$$
$$x = \quad ay + bz,$$

so reduciert sich dieser Teiler auf die Form $py^2 + 2qyz + rz^2$, und die angenommenen Werte von u und x sind so beschaffen, wie sie für die Transformation sein müssen, da $a\beta - \alpha b = 1$ ist.

277.

Nun mufs offenbar, wenn es je nach den verschiedenen trinären Formen von Δ, welche einem und demselben trinären Werte von c entsprechen, verschiedene Werte von $a, b, a', b', \ldots$ gäbe, wenigstens eine der beiden Gleichungen

$$p = A\alpha^2 - 2Ba\alpha + Ca^2$$
$$r = A\beta^2 - 2Bb\beta + Cb^2$$

zwei Lösungen besitzen. Da aber die Gröfse $Ay'^2 - 2By'z' + Cz'^2$ im Allgemeinen $py^2 - 2qyz + rz^2$ äquivalent ist, so mufs wenigstens eine der beiden Gleichungen

$$p = py^2 - 2qyz + rz^2$$
$$r = py^2 - 2qyz + rz^2$$

zwei Lösungen zulassen. Da nun aber die rechten Seiten auf den einfachsten Ausdruck gebracht sind, so sind p und r die kleinsten Zahlen, welche die Formel $py^2 - 2qyz + rz^2$ enthält, und es giebt nur sehr wenig Fälle, in denen eine dieser Zahlen auf zweierlei

Weise in dieser Formel enthalten ist. Diese Fälle sind diejenigen, in denen die quadratischen Teiler ambig sind, und zwar giebt es deren nur drei, nämlich 1) wenn $p = r$, 2) wenn $2q = p$ oder $= r$, 3) wenn $q = 0$ ist.

278.

Übrigens kann man bei diesen verschiedenen Fällen unmittelbar einsehen, daſs es zwei einem und demselben trinären Werte von c entsprechende trinäre Formen des Teilers Δ giebt oder geben kann.

1) Ist nämlich $p = r$, so können die beiden unbestimmten Gröſsen y und z mit einander vertauscht werden, und es besitzt somit der Teiler Δ gleichzeitig die beiden trinären Formen:

$$\Delta = (my + nz)^2 + (m'y + n'z)^2 + (m''y + n''z)^2$$
$$\Delta = (ny + mz)^2 + (n'y + m'z)^2 + (n''y + m''z)^2.$$

Diese beiden Formen sind von einander verschieden, wofern nicht

$$\Delta = (my + nz)^2 + (ny + mz)^2 + (m'y \pm m'z)^2$$

ist; denn alsdann würde eine Vertauschung von y und z in den drei Quadraten, aus denen Δ besteht, keine Änderung hervorbringen. Unter dieser Annahme würde der Wert von c sein:

$$c = (m^2 - n^2)^2 + (m'n \mp m'm)^2 + (m'm \mp m'n)^2,$$

und da diese drei Glieder durch $(n \mp m)^2$ teilbar sind, so muſs man $n \mp m = 1$ setzen, wodurch man erhält:

$$c = (n \pm m)^2 + m'^2 + m'^2.$$

Ist nun zugleich $y \pm z = y'$, so geht der Wert von Δ über in:

$$(my' + z)^2 + (ny' \mp z)^2 + m'^2y'^2 = 2z^2 \mp 2zy' + \frac{c+1}{2}y'^2.$$

Diese Form kann aber mit der angenommenen Form

$$py^2 + 2qyz + pz^2$$

nur dann übereinstimmen, wenn man $p = 2 = \frac{1}{2}(c+1)$ oder $c = 3$ setzt, ein Fall, von dem man absehen kann, da alsdann der Teiler $2y^2 + 2yz + 2z^2$ nur die eine trinäre Form $y^2 + (y+z)^2 + z^2$ annehmen kann.

2) Ist $r = 2q$ oder $\Delta = py^2 + 2qyz + 2qz^2$, so ergiebt die einfache Substitution von $y' - z$ für y:

$$\Delta = py'^2 - 2(p-q)y'z + pz^2.$$

Diese Form stimmt mit der des vorhergehenden Falles überein. Man erhält also dann zwei verschiedene trinäre Formen, auſser wenn $p = 2$ oder $2q = 2$ ist. Ist $p = 2$, so hat man, da $2q$ nicht gröſser



sein kann als 2, notwendig auch $2q = 2$, und dies führt auf den Fall $c = 3$ zurück. Ist $2q = 2$, so kann der Teiler

$$\Delta = py^2 + 2yz + 2z^2$$

nur auf folgende Weise in drei Quadrate zerlegt werden:

$$\Delta = ((a+1)y + z)^2 + (ay - z)^2 + b^2y^2,$$

und diese ändert sich nicht, wenn man $-y-z$ für z setzt. Es giebt daher in diesem Falle nur eine trinäre Form von Δ, welche dem gegebenen trinären Werte von c entspricht.

3) Ist endlich $q = 0$ oder $\Delta = py^2 + rz^2$, so kann man offenbar das Vorzeichen einer der Unbestimmten nach Belieben ändern, so dafs man gleichzeitig die beiden Formen erhält:

$$\Delta = (my + nz)^2 + (m'y + n'z)^2 + (m''y + n''z)^2$$
$$\Delta = (my - nz)^2 + (m'y - n'z)^2 + (m''y - n''z)^2,$$

und diese entsprechen demselben trinären Werte von c.

Die beiden Formen von Δ sind von einander verschieden, wofern nicht

$$\Delta = (my + nz)^2 + (my - nz)^2 + (m'z)^2$$

ist. In diesem Falle würde der entsprechende Wert von c sein:

$$c = (2mn)^2 + (m'm)^2 + (m'm)^2,$$

und damit dieser keinen allen seinen Gliedern gemeinsamen Faktor besitze, mufs man $m = 1$ setzen, wodurch sich $\Delta = 2y^2 + rz^2$ ergiebt. Mithin giebt es, den einen Fall $p = 2$ oder $r = 2$ ausgenommen, stets zwei trinäre Formen des Teilers Δ, welche demselben gegebenen trinären Werte von c entsprechen.

279.

Aus dieser Untersuchung ergiebt sich, wenn die trinäre Form $c = f^2\mu^2\nu^2 + g^2\nu^2\lambda^2 + h^2\lambda^2\mu^2$ gegeben ist, und der entsprechende trinäre Teiler der Formel $t^2 + cu^2$ gefunden werden soll, das Folgende:

1) Dieser Teiler wird durch die Formel $\Delta = \lambda^2x^2 + \mu^2x'^2 + \nu^2x''^2$ gegeben, in welcher die unbestimmten Gröfsen x, x', x'' mit Hülfe der Gleichung $fx + gx' + hx'' = 0$ auf zwei zu reducieren sind.

2) Auf welche Weise auch diese Reduktion durch Einführung zweier beliebigen Veränderlichen y und z an Stelle der drei x, x', x'' geschehen möge, das Resultat wird stets, auf den einfachsten Ausdruck gebracht, denselben quadratischen Teiler $py^2 + 2qyz + rz^2$ ergeben.

3) Gehört dieser Teiler zur Klasse der ambigen Teiler, d. h. gehört er zu einem der drei Fälle $p = r$, $2q = p$, $q = 0$, und ist zugleich die kleinere der beiden Zahlen p und r weder gleich 1 noch gleich 2, so besitzt der quadratische Teiler Δ stets zwei, aber nicht mehr wie zwei, dem gegebenen Werte von c entsprechende trinäre Formen.

4) Ist der quadratische Teiler Δ nicht ambig, oder ist, im Falle er ambig ist, sein kleinster Koefficient 1 oder 2, so giebt es stets nur eine trinäre Form des Teilers Δ, welche einem gegebenen trinären Werte von c entspricht.

§ 3.

Auf die trinären quadratischen Teiler bezügliche Sätze.

280.

Satz 1. Ist c eine Primzahl oder das Doppelte einer Primzahl, so können zwei verschiedene trinäre Formen von c nicht einem und demselben trinären Teiler der Formel $t^2 + cu^2$ entsprechen.

Die eine der gegebenen Formen sei:

$$c = F^2 + (K^2 + L^2)\vartheta^2,$$

die andere:

$$c = F'^2 + (K'^2 + L'^2)\vartheta'^2,$$

wo K und L sowohl als K' und L' prim zu einander sind. Entspräche diesen beiden gegebenen trinären Formen von c gleichzeitig derselbe quadratische Teiler Δ, so müfsten die beiden Zahlen $K^2 + L^2$ und $K'^2 + L'^2$ zu diesem Teiler gehören (No. 274). Setzte man also:

$$K^2 + L^2 = \pi, \qquad K'^2 + L'^2 = \pi',$$

so müfste sein (No. 233):

$$\pi\pi' = y^2 + cz^2.$$

Multipliciert man diese Gleichung mit $\vartheta^2\vartheta'^2$, und setzt die Werte $\pi\vartheta^2 = c - F^2$, $\pi'\vartheta'^2 = c - F'^2$ ein, so erhält man:

$$(c - F^2)(c - F'^2) = (y^2 + cz^2)\vartheta^2\vartheta'^2,$$

oder:

$$c^2 - c(F^2 + F'^2) + F^2F'^2 = y^2\vartheta^2\vartheta'^2 + cz^2\vartheta^2\vartheta'^2,$$

und hieraus erkennt man, dafs $F^2F'^2 - y^2\vartheta^2\vartheta'^2$ durch c teilbar sein mufs.

Ist erstens c eine Primzahl, so mufs einer der Faktoren

$FF' - y\vartheta\vartheta'$, $FF' + y\vartheta\vartheta'$ durch c teilbar sein, und da das Vorzeichen von y beliebig ist, so kann man

$$FF' - y\vartheta\vartheta' = cu \quad \text{oder} \quad y\vartheta\vartheta' = FF' - cu$$

setzen.

Ist zweitens c das Doppelte einer Primzahl, so mufs stets einer dieser Faktoren durch c teilbar sein. Da aber ihre Differenz $2y\vartheta\vartheta'$ eine gerade Zahl ist, so müssen, wenn ihr Produkt durch die Zahl c teilbar ist, notwendig alle beiden Faktoren gerade sein. Mithin ist $FF' - y\vartheta\vartheta'$ durch c teilbar und man kann daher ebenso

$$y\vartheta\vartheta' = FF' - cu$$

setzen.

Substituiert man diesen Wert in die vorhergehende Gleichung und dividiert das Ganze durch c, so erhält man:

$$c - F^2 - F'^2 = z^2\vartheta^2\vartheta'^2 + cu^2 - 2uFF',$$

oder:

$$c - F^2 = (F' - Fu)^2 + (c - F^2)u^2 + z^2\vartheta^2\vartheta'^2.$$

Da die Gröfse $c - F^2$ positiv ist, so kann diese Gleichung nur bestehen, wenn $u = 0$ ist. Dies giebt $y\vartheta\vartheta' = FF'$ und

$$c = F^2 + F'^2 + z^2\vartheta^2\vartheta'^2.$$

Wir müssen jetzt die drei Fälle, welche je nach den verschiedenen Formen von c eintreten können, betrachten.

281.

1) Ist c von der Form $4n + 1$, so müssen von den drei Quadraten, aus denen der trinäre Wert von c besteht, notwendig zwei gerade und eins ungerade sein. Nimmt man für F^2 und F'^2 die ungeraden Quadrate, welche in den beiden trinären Werten von c vorkommen, so ist die Gleichung $c = F^2 + F'^2 + z^2\vartheta^2\vartheta'^2$ unmöglich, da in diesem trinären Werte von c zwei ungerade Quadrate auftreten. Mithin können die beiden gegebenen trinären Werte von c nicht einem und demselben quadratischen Teiler der Formel $t^2 + cu^2$ entsprechen.

2) Ist c von der Form $4n + 2$, so müssen von den drei Quadraten, aus denen jede trinäre Form von c besteht, notwendig zwei ungerade und eins gerade sein. Sind F^2 und F'^2 die beiden geraden Quadrate in den beiden trinären Werten von c, so ist die Gleichung $c = F^2 + F'^2 + z^2\vartheta^2\vartheta'^2$ ebenfalls unmöglich. Mithin gilt der allgemeine Satz auch für den Fall, dafs c von der Form $4n + 2$.

3) Ist endlich c von der Form $8n + 3$, so sind die drei Quadrate, aus denen jede trinäre Form von c besteht, ungerade, und



es scheint daher, als ob die Gleichung $c = F^2 + F'^2 + z^2\vartheta^2\vartheta'^2$ in dieser Hinsicht nicht unmöglich wäre. Wir müssen daher auf eine weitere Teilung dieses dritten Falles zurückgehen.

Die Form $8n + 3$, zu welcher c gehört, teilt sich wieder in drei andere $24k+3$, $24k+11$, $24k+19$. Da die erstere $24k+3$ durch 3 teilbar ist und wir von dem Falle $c = 3$ abgesehen haben, so kann dieselbe nicht stattfinden, wenn c eine Primzahl ist. Wir haben daher nur noch die beiden andern Formen von c zu betrachten.

Zunächst bemerken wir, daſs jede ungerade Zahl, wenn sie in Bezug auf die Vielfachen von 12 betrachtet wird, von einer der Formen ist:

$$12n + 1,\ 12n + 3,\ 12n + 5,\ 12n + 7,\ 12n + 9,\ 12n + 11.$$

Das Quadrat einer jeden ungeraden Zahl ist daher von einer der Formen: $24n + 1$ und $24n + 9$ (oder vielmehr $72n + 9$), und zwar gilt die letztere, wenn die Zahl durch 3 teilbar ist, die erstere, wenn dies nicht der Fall.

1) Ist hiernach c von der Form $24k + 11$, so müssen von den drei Quadraten, aus denen c besteht, notwendig zwei von der Form $24n + 1$ und eins von der Form $24n + 9$ sein, da keine andere Verbindung $24k + 11$ als Summe der drei Quadrate ergeben kann. Nehmen wir also in den beiden gegebenen trinären Formen für F^2 und F'^2 die Quadrate von der Form $24n + 9$, so ist die Gleichung $c = F^2 + F'^2 + z^2\vartheta^2\vartheta'^2$ unmöglich, da von den drei Quadraten der rechten Seite zwei von der Form $24n + 9$ sind.

2) Ist c von der Form $24k + 19$, so sind von den drei Quadraten, aus denen jede trinäre Form von c besteht, zwei von der Form $24n + 9$ und eins von der Form $24n + 1$. Nimmt man also für F^2 und F'^2 die Quadrate, welche in den beiden gegebenen trinären Formen von c die Form $24n + 1$ besitzen, so ist die Gleichung $c = F^2 + F'^2 + z^2\vartheta^2\vartheta'^2$ ebenfalls unmöglich.

Mithin gilt der angegebene Satz in allen Fällen.

282.

Bemerkung. Es ist leicht zu zeigen, daſs derselbe Satz auch gilt, wenn c oder $\frac{1}{2}c$ irgend eine Potenz einer Primzahl α ist.

Es sei nämlich $c = \alpha^m$ oder $c = 2\alpha^m$. Da das Produkt der beiden Faktoren $FF' + y\vartheta\vartheta'$ und $FF' - y\vartheta\vartheta'$ durch α^m teilbar ist, so muſs man, wenn $m = \mu + \nu$ gesetzt wird, haben:

$$FF' + y\vartheta\vartheta' = \alpha^\nu t$$
$$FF' - y\vartheta\vartheta' = \alpha^\mu u.$$

Dies giebt:

$$2FF' = \alpha^\nu t + \alpha^\mu u.$$

Ist daher eine der beiden Zahlen μ und ν von 0 verschieden, so mufs wenigstens eine der beiden Zahlen F und F' durch α teilbar sein. Da aber jede gegebene trinäre Form von c eine eigentliche trinäre Form ist, deren Glieder nicht sämtlich durch dieselbe Zahl teilbar sind, so mufs offenbar in jeder Form wenigstens ein Glied vorkommen, welches nicht durch α teilbar ist. Nehmen wir an, dafs F^2 und F'^2 in den beiden Formen derartige Glieder sind, so mufs, weil alsdann FF' nicht durch α teilbar ist, einer der beiden Exponenten μ und ν gleich 0 sein. Setzt man $\nu = 0$ oder $\mu = m$, so erhält man:

$$FF' - y\vartheta\vartheta' = \alpha^m u.$$

Ist c ungerade, so ist die rechte Seite gleich cu; und ist c gerade, so kann man, weil alsdann die linke Seite gerade sein mufs, ebenfalls

$$FF' - y\vartheta\vartheta' = cu$$

setzen. Der übrige Teil des Beweises bleibt derselbe, wie oben. Daraus erkennt man, dafs der allgemeine Satz auch gilt, wenn c oder $\frac{1}{2}c$ eine Potenz einer Primzahl ist.

Man mufs jedoch hiervon den Fall $c = 3^{2m+1}$ ausnehmen. Derselbe würde einen besonderen Beweis erfordern, weil er in der Form $24k + 3$, von der wir abgesehen haben, enthalten ist.

283.

Satz 2. Ist c eine Primzahl oder das Doppelte einer Primzahl, so hat die Formel $t^2 + cu^2$ ebenso viele trinäre quadratische Teiler, als es trinäre Formen der Zahl c giebt.

Denn jeder trinäre Teiler der Formel $t^2 + cu^2$ entspricht einer sich unmittelbar aus ihm ergebenden trinären Form von c, und umgekehrt führt jede trinäre Form von c zu einem entsprechenden trinären Teiler der Formel $t^2 + cu^2$. Gäbe es also von beiden nicht eine gleiche Anzahl, so müfsten entweder zwei trinäre Formen von c demselben quadratischen Teiler der Formel $t^2 + cu^2$, oder zwei verschiedene quadratische Teiler derselben trinären Form von c entsprechen. Die zweite Annahme ist für keinen Wert von c richtig (No. 274), und die erste kann dem vorhergehenden Satze zufolge nicht stattfinden, da c eine Primzahl oder das Doppelte einer Primzahl ist. Also u. s. w.

284.

Satz 3. Ist c eine Primzahl oder das Doppelte einer Primzahl, so kann jeder trinäre Teiler der Formel $t^2 + cu^2$ nur auf eine einzige Weise in drei Quadrate zerlegt werden, er kann, mit andern Worten, nur eine einzige trinäre Form haben.

Denn hätte ein und derselbe quadratische Teiler der Formel $t^2 + cu^2$ mehrere trinäre Formen, so müſsten die verschiedenen trinären Formen nach dem vorigen Satze demselben trinären Werte von c entsprechen. Wir haben aber (No. 277) bewiesen, daſs ein gegebener trinärer Wert von c zwei verschiedenen trinären Formen desselben quadratischen Teilers nur dann entsprechen kann, wenn der letztere von einer der Formen

$$py^2 + rz^2, \quad py^2 + 2qyz + 2qz^2, \quad py^2 + 2qyz + pz^2$$

ist, und wenn zu gleicher Zeit die äuſseren Koefficienten beide gröſser als 2 sind. In allen diesen Fällen kann aber, wie leicht zu sehen, die Zahl c, welche der Reihe nach durch pr, $2pq - q^2$, $p^2 - q^2$ dargestellt wird, weder eine Primzahl noch das Doppelte einer Primzahl sein.

Bemerkung. Dieser Satz würde ebenfalls richtig sein, wenn c oder $\frac{1}{2}c$ eine Potenz einer Primzahl wäre. Er enthält somit eine **Eigenschaft**, welche **ausschlieſslich** den **Potenzen der Primzahlen** und dem Doppelten derselben zukommt, und die daher dazu dienen kann, diese Zahlen von allen andern zu unterscheiden.

285.

Satz 4. Ist die Zahl N in einem trinären Teiler der Formel $t^2 + cu^2$ enthalten, so ist auch umgekehrt die Zahl c in einem trinären Teiler der Formel $t^2 + Nu^2$ enthalten, und ferner sind die entsprechenden trinären Werte von N und c dieselben, mag man N als Teiler von $t^2 + cu^2$ oder c als Teiler von $t^2 + Nu^2$ betrachten.

Setzt man ebenso wie oben:

$$c = f^2\mu^2\nu^2 + g^2\nu^2\lambda^2 + h^2\lambda^2\mu^2,$$

so ist der entsprechende trinäre Teiler:

$$\Delta = \lambda^2 x^2 + \mu^2 x'^2 + \nu^2 x''^2,$$

vorausgesetzt, daſs der Bedingung



$$0 = fx + gx' + hx''$$

genügt wird. Ist nun N irgend eine, in dem Teiler Δ enthaltene Zahl, so mufs man gleichzeitig haben:

$$N = \lambda^2 m^2 + \mu^2 m'^2 + \nu^2 m''^2$$
$$0 = fm \quad + gm' \quad + hm''.$$

Wenn man zu diesem trinären Werte von N den entsprechenden trinären Teiler von $t^2 + Nu^2$ sucht, so mufs man die gemeinschaftlichen Teiler betrachten, welche je zwei der Gröfsen m, m', m'' haben können. Ist α der gemeinsame Teiler von m' und m'', β der von m'' und m, γ der von m und m', so kann man also setzen:

$$N = \lambda^2\beta^2\gamma^2 n^2 + \mu^2\alpha^2\gamma^2 n'^2 + \nu^2\alpha^2\beta^2 n''^2$$
$$0 = f\beta\gamma n \quad + g\alpha\gamma n' \quad + h\alpha\beta n''.$$

Wird die zweite von diesen Gleichungen auf die Form

$$\frac{f}{\alpha} n + \frac{g}{\beta} n' + \frac{h}{\gamma} n'' = 0$$

gebracht, so sieht man, dafs $\frac{f}{\alpha}, \frac{g}{\beta}, \frac{h}{\gamma}$ ganze Zahlen sein müssen; denn wenn n und α einen gemeinsamen Teiler hätten, so würden auch die drei Zahlen m, m', m'' einen solchen besitzen, welchen Fall wir stets ausgeschlossen haben. Ebenso zeigt man, dafs auch n' und β, sowie n'' und γ keinen gemeinschaftlichen Teiler haben. Ist daher $f = \alpha f'$, $g = \beta g'$, $h = \gamma h'$, so geht die vorige Gleichung über in

$$f'n + g'n' + h'n'' = 0.$$

Nennen wir Γ den trinären Teiler von $t^2 + Nu^2$, welcher dem Werte $N = \lambda^2\beta^2\gamma^2 n^2 + \mu^2\gamma^2\alpha^2 n'^2 + \nu^2\alpha^2\beta^2 n''^2$ entspricht, so erhalten wir die beiden simultanen Gleichungen:

$$\Gamma = \alpha^2 x^2 + \beta^2 x'^2 + \gamma^2 x''^2$$
$$0 = \lambda n x + \mu n' x' + \nu n'' x''.$$

Substituiert man aber die Werte von f, g, h in den Ausdruck von c, so ergiebt sich:

$$c = \alpha^2\mu^2\nu^2 f'^2 + \beta^2\nu^2\lambda^2 g'^2 + \gamma^2\lambda^2\mu^2 h'^2,$$

ein Wert, der in Γ enthalten ist, wenn man

$$x = \mu\nu f', \; x' = \nu\lambda g', \; x'' = \lambda\mu h'$$

setzt und zugleich die Bedingung

$$0 = \lambda n x + \mu n' x' + \nu n'' x''$$

erfüllt ist. Diese reduciert sich aber auf:

$$0 = f'n + g'n' + h'n'';$$

sie ist also in der That erfüllt, und damit ist der Satz in seiner ganzen Allgemeinheit bewiesen.

286.

Beispiel. Die Formel $t^2 + 65u^2$ besitzt den trinären Teiler:

$$9y^2 + 8yz + 9z^2 = (2y - z)^2 + (2y + 2z)^2 + (y + 2z)^2,$$

und diesem entspricht der Wert von c:

$$c = 6^2 + 2^2 + 5^2.$$

Ist $y = 5$ und $z = -2$, so erhält man die Zahl:

$$N = 181 = 12^2 + 6^2 + 1.$$

Sucht man nun mit Hülfe dieses Wertes den entsprechenden trinären Teiler von $t^2 + 181u^2$, so findet man für diesen Teiler:

$$5y^2 + 4yz + 37z^2 = y^2 + (6z)^2 + (2y + z)^2.$$

Diese Formel enthält aber die Zahl 65, wenn man $y = 2$ und $z = 1$ setzt, und die trinäre Form ist $65 = 2^2 + 6^2 + 5^2$, während der trinäre Wert von N, welcher sich aus demselben Teiler ergiebt, der folgende ist: $181 = 12^2 + 6^2 + 1^2$. Man ersieht hieraus, dafs 65 und 181 auseinander in derselben trinären Form hervorgehen, mag man nun 65 als Teiler von $t^2 + 181u^2$ oder 181 als Teiler von $t^2 + 65u^2$ betrachten, und dies ist in Übereinstimmung mit unserem Satze.

287.

Satz 5. Wenn der zur Formel $t^2 + cu^2$ gehörige quadratische Teiler $\Delta = py^2 + 2qyz + rz^2$ mehrere trinäre Formen annehmen kann, und wenn man in diesen verschiedenen Formen für y und z die bestimmten Werte $y = f$, $z = g$ setzt, so werden die trinären Formen, welche sich daraus für die Zahl $N = pf^2 + 2qfg + rg^2$ ergeben, sämtlich von einander verschieden sein, wenigstens so lange N gröfser ist als $\frac{2}{3}c$.

Sucht man nämlich direkt die Fälle zu bestimmen, in denen zwei trinäre Formen des Teilers Δ für die bestimmte Zahl N einen und denselben trinären Wert ergeben, so findet man, dafs N nicht gröfser sein kann als $\frac{2}{3}c$. Dies wollen wir jetzt auseinandersetzen.

Wir setzen voraus, dafs der Teiler $\Delta = py^2 + 2qyz + rz^2$ die beiden trinären Formen

$$\Delta = (my + nz)^2 + (m'y + n'z)^2 + (m''y + n''z)^2$$
$$\Delta = (\mu y + \nu z)^2 + (\mu' y + \nu' z)^2 + (\mu'' y + \nu'' z)^2$$

annehmen könne, so dafs gleichzeitig ist:

$$\begin{aligned} p &= m^2 + m'^2 + m''^2 = \mu^2 + \mu'^2 + \mu''^2 \\ q &= mn + m'n' + m''n'' = \mu\nu + \mu'\nu' + \mu''\nu'' \\ r &= n^2 + n'^2 + n''^2 = \nu^2 + \nu'^2 + \nu''^2. \end{aligned}$$

Sollen die besonderen Werte $y = f$, $z = g$, für welche der Teiler Δ gleich N wird, so beschaffen sein, dafs sich die beiden trinären Formen von Δ auf eine einzige trinäre Form von N reducieren, so mufs sein:

$$\begin{aligned} mf + ng &= \mu f + \nu g \\ m'f + n'g &= \mu' f + \nu' g \\ m''f + n''g &= \mu'' f + \nu'' g. \end{aligned}$$

Denn die beiden trinären Formen, welche zusammenfallen sollen, können so geordnet werden, dafs die gleichen Glieder an derselben Stelle stehen und die Quadratwurzeln der letzteren dasselbe Zeichen haben.

Da ferner f und g prim zu einander sind, so kann man den vorstehenden drei Gleichungen allgemein genügen, wenn man drei unbestimmte Gröfsen a, a', a'' annimmt und setzt:

$$\begin{aligned} \mu &= m - ag, & \mu' &= m' - a'g, & \mu'' &= m'' - a''g \\ \nu &= n + af, & \nu' &= n' + a'f, & \nu'' &= n'' + a''f. \end{aligned}$$

Setzt man diese Werte in die Werte von p, q, r ein, so erhält man die drei Gleichungen:

$$\left.\begin{aligned} \tfrac{1}{2}g(a^2 + a'^2 + a''^2) - ma - m'a' - m''a'' &= 0 \\ \tfrac{1}{2}f(a^2 + a'^2 + a''^2) + na + n'a' + n''a'' &= 0 \end{aligned}\right\} (A)$$

$$\left.\begin{aligned} fg(a^2 + a'^2 + a''^2) + g(na + n'a' + n''a'') \\ - f(ma + m'a' + m''a'') \end{aligned}\right\} = 0.$$

Wie man sieht, ist die dritte eine Folge der beiden andern, so dafs wir nur diese in Betracht zu ziehen brauchen.

Wie man auch den Gleichungen (A) genügen möge, es werden immer die Werte von f und g eine Zahl

$$N = pf^2 + 2qfg + rg^2$$

von der Beschaffenheit bestimmen, dafs, wenn man darauf die beiden trinären Formen von Δ anwendet, dieselben sich auf einen einzigen trinären Wert von N reducieren. Wir suchen daher den gröfsten Wert von N, für welchen diese Koincidenz stattfindet.

Zuerst bemerken wir, dafs, weil f und g nicht alle beide gerade

sein können, die Zahl $a^2 + a'^2 + a''^2$ den Gleichungen (A) zufolge gerade sein muſs. Ist also:

$$a^2 + a'^2 + a''^2 = 2k,$$

so erhält man:

$$f = -\frac{na + n'a' + n''a''}{k}, \quad g = \frac{ma + m'a' + m''a''}{k},$$

und hieraus folgt:

$$\begin{aligned} k(mf + ng) &= (m'n - mn')a' - (mn'' - m''n)a'' \\ k(m'f + n'g) &= (m''n' - m'n'')a'' - (m'n - mn')a \\ k(m''f + n''g) &= (mn'' - m''n)a - (m''n' - m'n'')a'. \end{aligned}$$

Die trinäre Form von c, welche dem trinären Teiler

$$(my + nz)^2 + (m'y + n'z)^2 + (m''y + n''z)^2$$

entspricht, ist:

$$c = (mn' - m'n)^2 + (m'n'' - m''n')^2 + (m''n - mn'')^2.$$

Setzt man zur Abkürzung:

$$m'n - mn' = \gamma, \quad m''n' - m'n'' = \alpha, \quad mn'' - m''n = \beta,$$

so daſs

$$c = \alpha^2 + \beta^2 + \gamma^2$$

wird, so geben die obigen Gleichungen:

$$\begin{aligned} k(mf + ng) &= \gamma a' - \beta a'' \\ k(m'f + n'g) &= \alpha a'' - \gamma a \\ k(m''f + n''g) &= \beta a - \alpha a'. \end{aligned}$$

Quadriert und addiert man diese Gleichungen, so erhält man:

$$k^2 N = (\gamma a' - \beta a'')^2 + (\alpha a'' - \gamma a)^2 + (\beta a - \alpha a')^2.$$

Da aber $c = \alpha^2 + \beta^2 + \gamma^2$ und $2k = a^2 + a'^2 + a''^2$ ist, so reduciert sich die rechte Seite, wie leicht zu sehen, auf:

$$2ck - (\alpha a + \beta a' + \gamma a'')^2,$$

so daſs man hat:

$$k^2 N = 2ck - (\alpha a + \beta a' + \gamma a'')^2.$$

Dieses Resultat zeigt, daſs die Grenze von N gleich $\frac{2c}{k}$ ist, und daſs N diese Grenze nur dann erreichen kann, wenn $\alpha a + \beta a' + \gamma a'' = 0$ ist.

288.

Die Grenze von N ist um so gröſser, je kleiner k ist; wir wollen daher zusehen, welches der kleinste Wert von k ist.

Die Werte, welche a, a', a'' besitzen müssen, damit $a^2 + a'^2 + a''^2$ möglichst klein und eine gerade Zahl sei, sind 0, 1, 1. Alsdann aber würde $f = -n' - n''$, $g = m' + m''$ sein, und die Form

$$(\mu y + \nu z)^2 + (\mu' y + \nu' z)^2 + (\mu'' y + \nu'' z)^2$$

würde sich von der Form

$$(my + nz)^2 + (m'y + n'z)^2 + (m''y + n''z)$$

nur durch die Reihenfolge der Glieder unterscheiden, was gegen unsere Annahme ist.

Ebenso kann man nicht $a = 0$, $a' = 0$, $a'' = 2$ setzen, weil alsdann die beiden trinären Formen von Δ sich auf eine und dieselbe Form reducieren würden. Der kleinste Wert von k findet also statt für $a = 1$, $a' = 1$, $a'' = 2$. Alsdann ist $k = 3$, und die gesuchte Grenze ist $N < \frac{2}{3}c$, übereinstimmend mit unserm Satze.

289.

Damit N diese Grenze erreiche, mufs

$$\alpha + \beta + 2\gamma = 0 \quad \text{oder} \quad \alpha = -\beta - 2\gamma$$

und daher

$$c = \alpha^2 + \beta^2 + \gamma^2 = 2(\beta + \gamma)^2 + 3\gamma^2$$

sein. Da aber $N = \frac{2}{3}c$ ist, so mufs sich c durch 3 teilen lassen. Setzt man also $\beta + \gamma = 3\delta$, so erhält man:

$$c = 3\gamma^2 + 18\delta^2.$$

Hierin mufs γ eine ungerade Zahl sein, da sonst N durch 4 teilbar sein müfste, was jedoch bei den Zahlen, welche eine trinäre Form annehmen, nicht stattfinden kann.

Diese Resultate lassen sich leicht bestätigen. Denn zufolge des gefundenen Wertes von c ist einer der quadratischen Teiler von $t^2 + cu^2$:

$$\Delta = (2\gamma^2 + 12\delta^2)y^2 + (2\gamma^2 + 12\delta^2)yz + \left(\frac{\gamma^2 + 3}{2} + 3\delta^2\right)z^2.$$

Derselbe zerlegt sich auf folgende zwei Arten in drei Quadrate:

$$\left((\gamma + 2\delta)y + \left(\frac{1}{2}\gamma + \frac{1}{2} + \delta\right)z\right)^2 + \left((\gamma - 2\delta)y + \left(\frac{1}{2}\gamma - \frac{1}{2} - \delta\right)z\right)^2 + (2\delta y + (\delta - 1)z)^2$$

$$\left((\gamma + 2\delta)y + \left(\frac{1}{2}\gamma - \frac{1}{2} + \delta\right)z\right)^2 + \left((\gamma - 2\delta)y + \left(\frac{1}{2}\gamma + \frac{1}{2} - \delta\right)z\right)^2 + (2\delta y + (\delta + 1)z)^2,$$

und diese zwei Formen reducieren sich auf eine einzige, wenn man $y = 1$, $z = 0$ setzt. Dies giebt $N = 2\gamma^2 + 12\delta^2 = \frac{2}{3}c$.

290.

Satz 6. Wenn die Zahl N auf m verschiedene Arten in einem oder mehreren quadratischen Teilern der Formel

$$t^2 + cu^2$$

enthalten ist, wenn sich ferner jeder dieser verschiedenen Teiler in n trinäre Formen zerlegen läfst, und somit die Zahl N, als Teiler der Formel $t^2 + cu^2$, mn trinäre Werte annimmt, so sind alle diese trinären Werte von einander verschieden, mit Ausnahme des Falles $N < \frac{2}{3}c$ und desjenigen, in welchem man der Gleichung $c^2 = y^2 + Nz^2$ genügen könnte, ohne dafs man $z = 0$ zu setzen brauchte.

Denn eine der trinären Formen von N läfst sich immer darstellen durch die Formel

$$N = \lambda^2 A^2 + \mu^2 B^2 + \nu^2 C^2,$$

wenn man annimmt, dafs der entsprechende Wert von c gleich

$$f^2\mu^2\nu^2 + g^2\nu^2\lambda^2 + h^2\lambda^2\mu^2$$

ist und zwischen den Zahlen A, B, C die Relation

$$fA + gB + hC = 0$$

besteht.

Ebenso läfst sich eine zweite trinäre Form von N durch die Formel

$$N = \lambda'^2 A'^2 + \mu'^2 B'^2 + \nu'^2 C'^2$$

darstellen, wenn man in ähnlicher Weise

$$c = f'^2\mu'^2\nu'^2 + g'^2\nu'^2\lambda'^2 + h'^2\lambda'^2\mu'^2 \text{ und } f'A' + g'B' + h'C' = 0$$

annimmt.

Sollen nun diese beiden trinären Werte von N identisch sein, so mufs man

$$\lambda A = \lambda' A', \quad \mu B = \mu' B', \quad \nu C = \nu' C'$$

setzen. Entnimmt man aus diesen Gleichungen die Werte von A', B', C' und setzt dieselben in die Gleichung

$$f'A' + g'B' + h'C' = 0$$

ein, so erhält man:

$$f'\mu'\nu' \cdot \lambda A + g'\nu'\lambda' \cdot \mu B + h'\lambda'\mu' \cdot \nu C = 0.$$

Verbindet man diese Gleichung mit der Gleichung

$$fA + gB + hC = 0,$$

so ergiebt sich:

$$\frac{\mu B}{\lambda A} = \frac{f'\mu'\nu' \,.\, h\lambda\mu - h'\lambda'\mu' \,.\, f\mu\nu}{h'\lambda'\mu' \,.\, g\nu\lambda - g'\nu'\lambda' \,.\, h\lambda\mu}$$

$$\frac{\nu C}{\lambda A} = \frac{g'\nu'\lambda' \,.\, f\mu\nu - f'\mu'\nu' \,.\, g\nu\lambda}{h'\lambda'\mu' \,.\, g\nu\lambda - g'\nu'\lambda' \,.\, h\lambda\mu}.$$

Wird zur Abkürzung gesetzt:

$$f\mu\nu = \alpha, \quad g\nu\lambda = \beta, \quad h\lambda\mu = \gamma$$
$$f'\mu'\nu' = \alpha', \quad g'\nu'\lambda' = \beta', \quad h'\lambda'\mu' = \gamma',$$

so dafs die trinären, den beiden identischen Werten von N entsprechenden Werte von c die folgenden sind:

$$c = \alpha^2 + \beta^2 + \gamma^2, \quad c = \alpha'^2 + \beta'^2 + \gamma'^2,$$

so erhält man:

$$\frac{\mu B}{\lambda A} = \frac{\alpha'\gamma - \alpha\gamma'}{\gamma'\beta - \gamma\beta'}$$
$$\frac{\nu C}{\lambda A} = \frac{\beta'\alpha - \beta\alpha'}{\gamma'\beta - \gamma\beta'}.$$

Nun können aber die drei Zahlen λA, μB, νC nicht durch einen und denselben Faktor teilbar sein. Nennt man also φ den gröfsten gemeinschaftlichen Teiler der drei Gröfsen

$$\alpha'\gamma - \alpha\gamma', \quad \beta'\alpha - \beta\alpha', \quad \gamma'\beta - \gamma\beta',$$

so ist:

$$\varphi\lambda A = \gamma'\beta - \gamma\beta'$$
$$\varphi\mu B = \alpha'\gamma - \alpha\gamma'$$
$$\varphi\nu C = \beta'\alpha - \beta\alpha'.$$

Hieraus folgt:

$$\varphi^2(\lambda^2A^2 + \mu^2B^2 + \nu^2C^2) = \varphi^2 N = (\gamma'\beta - \gamma\beta')^2 + (\alpha'\gamma - \alpha\gamma')^2 + (\beta'\alpha - \beta\alpha')^2.$$

Nun weifs man aber, vermöge einer bei derartigen Untersuchungen sich sehr häufig darbietenden Reduktion, dafs die rechte Seite nichts anderes ist als:

$$(\alpha^2 + \beta^2 + \gamma^2)(\alpha'^2 + \beta'^2 + \gamma'^2) - (\alpha\alpha' + \beta\beta' + \gamma\gamma')^2.$$

Daher ist, wenn man zur Abkürzung $\alpha\alpha' + \beta\beta' + \gamma\gamma' = \vartheta$ setzt:

$$\varphi^2 N = c^2 - \vartheta^2,$$

oder:

$$c^2 = \vartheta^2 + N\varphi^2.$$

Somit können zwei trinäre Formen von N nur dann identisch sein, wenn die Zahl N kleiner als c^2 und von der Beschaffenheit ist, dafs man der Gleichung $c^2 = y^2 + Nz^2$ genügen kann.

Dieses Resultat erleidet nur eine Ausnahme, wenn $\varphi = 0$ ist. Alsdann hat man $\frac{\gamma'}{\gamma} = \frac{\beta'}{\beta} = \frac{\alpha'}{\alpha}$, so dafs die Form $\alpha'^2 + \beta'^2 + \gamma'^2$ ganz und gar mit der Form $\alpha^2 + \beta^2 + \gamma^2$ zusammenfällt. In diesem Falle sind aber die beiden trinären Werte von N, welche man mit einander vergleicht, aus einem und demselben quadratischen Teiler

abgeleitet, da sie identischen trinären Werten von c entsprechen; mithin müssen diese beiden Werte von einander verschieden sein (No. 287), wofern nicht $N < \frac{2}{3} c$ ist. Fügt man daher diesen Ausnahmefall zu dem bereits gefundenen hinzu, so erhält man den allgemeinen Satz in der Fassung, in der wir ihn ausgesprochen haben.

291.

Um von diesem Satze eine Anwendung zu geben, betrachten wir die Formel $t^2 + 21u^2$ und ihren quadratischen Teiler

$$\Delta = 5y^2 + 4yz + 5z^2.$$

Derselbe kann die beiden trinären Formen annehmen:

$$(2y + z)^2 + y^2 + 4z^2$$
$$(y + 2z)^2 + z^2 + 4y^2.$$

In diesem Teiler ist die Zahl $17765 = 5 \cdot 11 \cdot 17 \cdot 19$ enthalten. Da diese von der Form $84x + 41$ ist, so kann sie (der Tafel IV zufolge) zu keinem andern quadratischen Teiler der Formel $t^2 + 21u^2$ gehören. Ferner mufs diese Zahl wegen der vier Faktoren, aus denen sie besteht, 2^3- oder 8-mal in dem Teiler $5y^2 + 4yz + 5z^2$ enthalten sein. In der That findet man, wenn man die Gleichung

$$17765 = 5y^2 + 4yz + 5z^2$$

auflöst, die folgenden acht Lösungen:

$$y = 52, \; -64, \; 31, \; -63, \; -1, \; -47, \; -24, \; -28$$
$$z = 15, \; 15, \; 40, \; 40, \; 60, \; 60, \; 65, \; 65.$$

Man würde sogar noch acht andere finden, jedoch würden dieselben kein neues Resultat ergeben, da der quadratische Teiler

$$5y^2 + 4yz + 5z^2$$

zu den ambigen Teilern gehört. Hiernach ergiebt von den acht gefundenen Lösungen eine jede zwei trinäre Formen von 17765, welche von einander verschieden sind, da die Gleichung $c^2 = y^2 + Nz^2$ offenbar nicht stattfinden kann. Mithin besitzt die Zahl 17765, als Teiler von $t^2 + 21u^2$ betrachtet, sechszehn verschiedene trinäre Formen. In der That findet man die folgenden Formen:

$119^2+60^2+2^2$	$119^2+52^2+30^2$	$102^2+65^2+56^2$	$86^2+63^2+80^2$
$58^2+120^2+1^2$	$82^2+104^2+15^2$	$9^2+130^2+28^2$	$17^2+126^2+40^2$
$113^2+64^2+30^2$	$106^2+65^2+48^2$	$111^2+40^2+62^2$	$73^2+60^2+94^2$
$34^2+128^2+15^2$	$17^2+130^2+24^2$	$102^2+80^2+31^2$	$34^2+120^2+47^2$



292.

Bemerkung. Ist N gerade und $> \frac{1}{4}c^2$, so kann die Gleichung $c^2 = y^2 + Nz^2$ nicht stattfinden, und der allgemeine Satz erleidet keine Ausnahme. Die Bedingung $N > \frac{2}{3}c$ ist nämlich dann von selbst erfüllt; ferner erfordert die Gleichung $c^2 = y^2 + Nz^2$, dafs $z = 1$ und $c^2 - y^2 = N$ sei; da aber N gerade ist, so mufs auch die linke Seite gerade sein. In diesem Falle würde jedoch die linke Seite durch 4 teilbar sein, während N nur durch 2 teilbar ist.

Bei derselben Voraussetzung $N > \frac{1}{4}c^2$ kann die Gleichung

$$N = c^2 - \vartheta^2$$

ebenfalls nicht stattfinden, wenn N von der Form $4n + 1$ und c gerade ist.

293.

Satz 7. Es sei $py^2 + 2qyz + rz^2$ ein quadratischer Teiler der Formel $t^2 + cu^2$ und p und c zu einander prime Zahlen. Ist dann die Zahl c ein Teiler von $t^2 + pu^2$, so ist auch c ein Teiler von $t^2 + Nu^2$, wo N irgend eine in der Formel

$$py^2 + 2qyz + rz^2$$

enthaltene Zahl ist.

Ist nämlich $N = p\alpha^2 + 2q\alpha\beta + r\beta^2$, so ist

$$pN = (p\alpha + q\beta)^2 + c\beta^2.$$

Nach Voraussetzung ist aber c ein Teiler von $t^2 + pu^2$; folglich giebt es eine ganze Zahl k von der Beschaffenheit, dafs $\frac{k^2 + p}{c}$ eine ganze Zahl ist, mithin ist auch $\frac{Nk^2 + Np}{c}$ eine ganze Zahl. Setzt man nun für Np seinen Wert, so erhält man:

$$\frac{(p\alpha + q\beta)^2 + Nk^2}{c} = e.$$

c und k sind aber prim zu einander; denn hätten sie einen gemeinschaftlichen Teiler ϑ, so müfsten, da $\frac{k^2 + p}{c}$ eine ganze Zahl ist, auch p und c denselben gemeinschaftlichen Teiler ϑ haben, was gegen die Voraussetzung ist. Demnach kann man $p\alpha + q\beta = kx + cu$ setzen, wodurch man erhält: $\frac{x^2 + N}{c} = e$. Folglich ist c ein Teiler von $x^2 + N$, oder allgemein ein Teiler der Formel $t^2 + Nu^2$.

294.

Bemerkung. Derselbe Satz würde auch gelten, wenn man nur voraussetzte, daſs der quadratische Teiler $py^2 + 2qyz + rz^2$ eine Zahl p' enthält, welche prim zu c und so beschaffen ist, daſs c ein Teiler von $t^2 + p'u^2$ ist. Denn durch eine Transformation kann man immer bewirken, daſs diese Zahl p' die Stelle des ersten Koefficienten p einnimmt (No. 233).

Wenn daher der quadratische Teiler $py^2 + 2qyz + rz^2$ eine einzige Zahl p' enthält, welche prim zu c und von solcher Beschaffenheit ist, daſs c ein Teiler von $t^2 + p'u^2$ wird, so besitzt jede in demselben quadratischen Teiler enthaltene Zahl N dieselbe Eigenschaft, so daſs c stets ein Teiler der Formel $t^2 + Nu^2$ ist.

295.

Satz 8. Wenn dagegen eine einzige in dem quadratischen Teiler $py^2 + 2qyz + rz^2$ enthaltene Zahl p' so beschaffen ist, daſs c nicht in $t^2 + p'u^2$ aufgeht, so ist jede in demselben quadratischen Teiler enthaltene Zahl N ebenfalls von der Art, daſs c kein Teiler sein kann von $t^2 + Nu^2$, wenigstens, sobald N und c zu einander prim vorausgesetzt werden.

Denn da c und N prim zu einander sind, so müſste, wenn c ein Teiler von $t^2 + Nu^2$ wäre, dem vorigen Satze zufolge auch c ein Teiler von $t^2 + p'u^2$ sein, was gegen die Voraussetzung ist.

296.

Zur Abkürzung werden wir einen **reciproken** Teiler jeden quadratischen Teiler der Formel $t^2 + cu^2$ nennen, welcher die Eigenschaft besitzt, daſs, wenn N irgend eine in diesem Teiler enthaltene Zahl bedeutet, auch umgekehrt c ein Teiler von $t^2 + Nu^2$ ist.

Im Gegensatz hierzu werden wir einen **nichtreciproken** Teiler jeden quadratischen Teiler nennen, welcher diese Eigenschaft entweder überhaupt nicht oder doch nur in Bezug auf einige besondere Zahlen N besitzt, die mit c einen gemeinschaftlichen Teiler haben.

Die Bedingungen dafür, daſs ein quadratischer Teiler reciprok sei oder nicht, sind durch die beiden vorhergehenden Sätze so scharf

angegeben, dafs man jederzeit sehr schnell und beinahe auf den ersten Blick entscheiden kann, ob ein gegebener quadratischer Teiler reciprok ist oder nicht.

297.

Als Beispiel wollen wir die Formel $t^2 + 69u^2$ betrachten, von welcher $5y^2 + 2yz + 14z^2$ ein quadratischer Teiler ist. Um zu erfahren, ob dieser Teiler reciprok ist, bemerke ich, dafs der Koefficient 5 prim zu 69 ist. Wir untersuchen also, ob 69 ein Teiler von $t^2 + 5u^2$ ist. Nun geht offenbar 69 in $8^2 + 5$ auf; mithin ist der in Rede stehende quadratische Teiler ein reciproker Teiler, d. h. wenn N irgend eine in der Formel $5y^2 + 2yz + 14z^2$ enthaltene Zahl ist, so kann man sicher sein, dafs 69 ein Teiler von $t^2 + Nu^2$ ist.

Da dieselbe Formel $t^2 + 69u^2$ einen zweiten quadratischen Teiler $6y^2 + 6yz + 13z^2$ besitzt, so nehme man, wenn man wissen will, ob dieser Teiler reciprok ist, die darin enthaltene zu 69 prime Zahl 13 und untersuche, ob 69 ein Teiler von $t^2 + 13u^2$ ist. Man sieht aber unmittelbar, dafs 3, ein Faktor von 69, kein Teiler von $t^2 + 13u^2$ ist, folglich kann es auch nicht 69 sein; mithin ist der quadratische Teiler $6y^2 + 6yz + 13z^2$ ein nichtreciproker Teiler.

Wir betrachten noch die Formel $t^2 + 45u^2$ und den quadratischen Teiler derselben $y^2 + 45z^2$. Um die Natur dieses Teilers zu bestimmen, nehme man den Koefficienten 1 des ersten Teilers und untersuche, ob 45 ein Teiler ist von $t^2 + u^2$. Man sieht aber sofort, dafs 3 kein Teiler ist von $t^2 + u^2$ (denn es werden t und u stets zu einander prim vorausgesetzt). Folglich kann auch 45 kein Teiler von $t^2 + u^2$ sein. Es ist daher der in Rede stehende Teiler ein nichtreciproker Teiler.

298.

Wir werden später zeigen, dafs die reciproken quadratischen Teiler nur diejenigen Zahlen enthalten, welche die trinäre Form annehmen können, d. h. die Zahlen von einer der Formen $8n + 1$, $8n + 2$, $8n + 3$, $8n + 5$, $8n + 6$. Berücksichtigt man nun die Gleichung $pr - q^2 = c$, so findet man leicht (wie in No. 225), dafs für jede dieser fünf Hauptformen von c die quadratischen Teiler von $t^2 + cu^2$ in zwei Arten zerfallen, welche sich nach den Vielfachen von 4 und 8 bestimmen, wie aus folgender Tafel ersichtlich ist:

Zahl c.	Teiler erster Art.	Teiler zweiter Art.
$8n+1$	$4n+1,\quad 8n+2$	$4n+3,\quad 8n+6$
$8n+5$	$4n+1,\quad 8n+6$	$4n+3,\quad 8n+2$
$8n+3$	$4n+2$	
$8n+2$	$8n+1,\quad 8n+3$ $c\quad,\quad c+4$	$8n+5,\quad 8n+7$ $c-4,\quad c+8$
$8n+6$	$8n+3,\quad 8n+5$ $c-4,\quad c+8$	$8n+1,\quad 8n+7$ $c\quad,\quad c+4$

Ist die Zahl c von der Form $8n+3$, so giebt es, wie man sieht, nur eine einzige Art von quadratischen Teilern, nämlich die Teiler von der Form $4n+2$. Gehört die Zahl c zu den Formen $8n+2$ oder $8n+6$, so kann man die entsprechenden geraden Teiler noch näher bestimmen. Dazu mufs man jede dieser Formen in zwei andere zerlegen; alsdann wird man an Stelle der beiden letzten Spalten der Tafel die folgenden vier erhalten:

$16n+2$	$8n+1,\quad 8n+3$ $16n+2,\quad 16n+6$	$8n+5,\quad 8n+7$ $16n+10,\quad 16n+14$
$16n+10$	$8n+1,\quad 8n+3$ $16n+10,\quad 16n+14$	$8n+5,\quad 8n+7$ $16n+2,\quad 16n+6$
$16n+6$	$8n+3,\quad 8n+5$ $16n+2,\quad 16n+14$	$8n+1,\quad 8n+7$ $16n+6,\quad 16n+10$
$16n+14$	$8n+3,\quad 8n+5$ $16n+6,\quad 16n+10$	$8n+1,\quad 8n+7$ $16n+2,\quad 16n+14.$

Mit Hülfe dieser Tafel erkennt man sofort, ob eine gegebene Zahl, welche ein Teiler von t^2+cu^2 ist, zur ersten oder zweiten Art gehört; man braucht dazu nur den Rest zu betrachten, welchen diese Zahl bei der Division durch 4, 8 oder 16 übrig läfst.

Da die quadratischen Teiler der zweiten Art immer Zahlen von der Form $8n+7$ enthalten, so können diese Teiler **niemals** trinär sein. Mithin müssen die reciproken Teiler sich stets unter den Teilern der ersten Art vorfinden.

299.

Satz 9. Ist c eine Primzahl oder das Doppelte einer Primzahl, so ist jeder quadratische Teiler erster Art der Formel $t^2 + cu^2$ ein reciproker Teiler.

1) Ist nämlich c eine Primzahl von der Form $4n + 1$, welche die beiden Formen $8n + 1$ und $8n + 5$ umfaſst, so haben wir bereits bewiesen, daſs, wenn N irgend ein Teiler der Formel $t^2 + cu^2$ von der Form $4n + 1$ ist, die Gleichung besteht $\left(\frac{N}{c}\right) = 1$. Demnach muſs c ein Teiler von $t^2 + Nu^2$ sein. Es ist daher der quadratische Teiler, welcher N enthält, ein reciproker Teiler. Folglich ist jeder quadratische Teiler der Formel $t^2 + cu^2$, welcher von der ersten Art ist, ein reciproker Teiler.

2) Ist c eine Primzahl von der Form $8n + 3$ und P irgend ein ungerader Teiler der Formel $t^2 + cu^2$, so hat man (No. 199) $\left(\frac{P}{c}\right) = 1$. Wegen der besonderen Beschaffenheit der Zahl c ist aber (No. 150) $\left(\frac{2}{c}\right) = -1$; mithin $\left(\frac{2P}{c}\right) = -1$. Somit ist c ein Teiler von $t^2 + 2Pu^2$ oder von $t^2 + Nu^2$, wenn N irgend ein Teiler der Formel $t^2 + cu^2$ von der Form $4n + 2$ ist. Demnach ist jeder quadratische Teiler dieser Formel, welcher die Form $4n + 2$ besitzt, ein reciproker Teiler.

3) Ist die Zahl $c = 2a$, wo a eine Primzahl von der Form $4n + 1$ ist, so folgt aus No. 200: $\left(\frac{N}{a}\right) = 1$, wenn N irgend einen Teiler der Formel $t^2 + cu^2$ oder $t^2 + 2au^2$ von der Form $8n + 1$ oder $8n + 3$ darstellt. Folglich ist a ein Teiler von $t^2 + Nu^2$, daher auch $2a$ oder c. Mithin ist jeder quadratische Teiler, welcher N enthält, d. h. jeder quadratische Teiler erster Art der Formel $t^2 + cu^2$ ein reciproker Teiler.

4) Ist endlich die Zahl $c = 2a$, wo a eine Primzahl von der Form $4n + 3$ ist, so haben wir in No. 200 bewiesen, daſs, wenn N irgend ein Teiler der Formel $t^2 + 2au^2$ von der Form $8n + 3$ oder $8n + 5$ ist, die Gleichung besteht: $\left(\frac{N}{a}\right) = -1$. Folglich ist a ein Teiler der Formel $t^2 + Nu^2$, daher auch $2a$ oder c. Mithin ist jeder quadratische Teiler, welcher N enthält, ein reciproker Teiler.

300.

Satz 10. Ist die Zahl c oder die Hälfte derselben eine zusammengesetzte Zahl, so giebt es unter den quadratischen

Teilern der Formel $t^2 + cu^2$, welche von erster Art sind, stets mindestens einen reciproken Teiler.

Dieser Satz sowie der vorige setzt voraus, dafs die Zahl c von einer der drei Formen $4n + 1$, $8n + 3$, $4n + 2$ sei. Wir begnügen uns jedoch damit, den eben angeführten Satz für die Zahlen von der Form $4n + 1$ zu beweisen, da die Schlufsreihe bei den andern Formen dieselbe bleibt.

Es sei also c eine zusammengesetzte Zahl von der Form $4n + 1$. Wenn man beweisen könnte, dafs es eine Primzahl N gäbe, welche ebenfalls von der Form $4n + 1$ und so beschaffen ist, dafs c ein Teiler von $t^2 + Nu^2$ wird, so würde daraus folgen (No. 198), dafs $\left(\frac{c}{N}\right) = 1$ oder dafs N ein Teiler der Formel $t^2 + cu^2$ ist, und dafs somit der quadratische Teiler dieser Formel, welcher N enthält, ein reciproker Teiler ist.

Zu diesem Zwecke zerlegen wir c in seine gleichen oder ungleichen Primfaktoren. Sind $\alpha, \alpha', \alpha'', \ldots$ die Faktoren von der Form $4n + 1$ und $\beta, \beta', \beta'', \ldots$ die Faktoren von der Form $4n + 3$, wobei die letzteren in gerader Anzahl vorhanden sein müssen, wenn c eine Zahl von der Form $4n + 1$ sein soll, so hat man

$$c = \alpha\alpha'\alpha'' \ldots \beta\beta'\beta'' \ldots$$

Damit nun c ein Teiler der Formel $t^2 + Nu^2$ sei, mufs der Reihe nach sein:

$$\left(\frac{N}{\alpha}\right) = 1, \quad \left(\frac{N}{\alpha'}\right) = 1, \quad \left(\frac{N}{\alpha''}\right) = 1, \cdots$$
$$\left(\frac{N}{\beta}\right) = -1, \quad \left(\frac{N}{\beta'}\right) = -1, \quad \left(\frac{N}{\beta''}\right) = -1, \cdots$$

Von diesen Bedingungen liefert jede, welche sich auf einen verschiedenen Nenner bezieht, im Allgemeinen mehrere lineare Werte von N (No. 195). Verbindet man diese Werte mit einander, um allen Gleichungen Genüge zu leisten, und bringt man sie sodann auf die Form $4n + 1$, so liefern dieselben eine grofse Menge von Formeln, von denen jede unendlich viele Primzahlen enthält. Es genügt aber eine einzige dieser Zahlen zur Bestimmung eines quadratischen Teilers der Formel $t^2 + cu^2$, und dieser ist reciprok, weil, wenn c ein Teiler von $t^2 + Nu^2$ ist, auch N in $t^2 + cu^2$ aufgeht.

301.

Bemerkung. Die reciproken Teiler der Formel $t^2 + cu^2$ bilden eine der Gruppen, in welche das vollständige System

der quadratischen Teiler dieser Formel zerfällt. Ist i die Anzahl der ungleichen Primfaktoren $\alpha, \alpha', \alpha'', \ldots \beta, \beta', \beta'', \ldots$, so stellt 2^i die Gesamtzahl der Gruppen dar; von diesen Gruppen ist eine, nämlich die, welche den Bedingungen

$$\left(\frac{N}{\alpha}\right) = 1, \quad \left(\frac{N}{\alpha'}\right) = 1, \cdots \quad \left(\frac{N}{\beta}\right) = -1, \cdots$$

Genüge leistet und von der ersten Art ist, die Gruppe der reciproken Teiler.

Ähnliche Resultate findet man in dem Falle, wo c von der Form $8n + 3$ oder von der Form $4n + 2$ ist.

302.

Satz 11. Jeder trinäre quadratische Teiler ist ein reciproker Teiler.

Denn ist Δ ein trinärer quadratischer Teiler der Formel $t^2 + cu^2$, und N irgend eine in Δ enthaltene Zahl, so ist c, wie wir gesehen haben, ein Teiler von $t^2 + Nu^2$ (No. 285). Mithin ist Δ ein reciproker Teiler.

303.

Die Umkehrung des vorhergehenden Satzes ist ebenfalls richtig, nämlich:

Jeder reciproke Teiler ist trinär.

Die Tafel VIII enthält nämlich die trinären Teiler der Formel $t^2 + cu^2$ für alle Werte von c von $c = 1$ an bis zu $c = 251$; man kann sich davon überzeugen, dafs es keinen reciproken Teiler der Formel $t^2 + cu^2$ giebt, der nicht darin enthalten wäre.

Dieser Satz kann also bis zu einer gegebenen Grenze L durch unmittelbare Bestätigung als richtig betrachtet werden, und es handelt sich darum zu zeigen, dafs er auch noch richtig bleibt, wenn c diese Grenze übersteigt.

Durch eine derartige Reciprocität hängt jede Formel $t^2 + cu^2$ mit denen, in welchen c kleiner ist, zusammen, so dafs die bekannten Eigenschaften der einen dazu dienen können, die Eigenschaften der andern zu beweisen.

Der allgemeine Satz, den wir zu beweisen haben, ist folgender:

304.

Satz 12. Jeder reciproke Teiler der Formel $t^2 + Nu^2$ ist ein trinärer Teiler, und zwar besitzt dieser Teiler so viele

trinäre Formen, als die Zahl 2^{i-1} Einheiten enthält. Dabei bedeutet i die Anzahl der ungeraden und ungleichen Primfaktoren, welche in N aufgehen.

Dieser Satz mufs als einer der **bemerkenswertesten** Sätze der Zahlentheorie betrachtet werden. Aus diesem Grunde geben wir für denselben zwei Beweise. Der erste stützt sich darauf, dafs es möglich ist, eine in einem gegebenen reciproken Teiler enthaltene und zwischen gegebenen Grenzen liegende Zahl zu finden, welche eine Primzahl oder das Doppelte einer Primzahl ist. Der andere ist von dieser Voraussetzung unabhängig.

305.

Erster Beweis.

Nehmen wir zunächst an, dafs N oder $\frac{1}{2}N$ eine Primzahl sei, so ist jeder Teiler der Formel $t^2 + Nu^2$, welcher von der ersten Art ist, ein reciproker Teiler (No. 299). Ist dieser Teiler

$$\Gamma = cy^2 + 2byz + az^2,$$

so behaupte ich, dafs Γ zu gleicher Zeit ein trinärer Teiler ist.

Denn der Eigenschaft dieses Teilers zufolge ist die Zahl N in einem quadratischen Teiler der Formel $t^2 + cu^2$ enthalten, welcher reciprok und somit trinär ist, weil c unterhalb der Grenze L liegt, bis zu welcher die Tafel als richtig erwiesen ist. Da ferner die Zahl N eine Primzahl oder das Doppelte einer Primzahl ist, so kann sie nur in einem einzigen der quadratischen Teiler von $t^2 + cu^2$ und darin nur auf eine einzige Weise enthalten sein. Ist daher

$$\Delta = py^2 + 2qyz + rz^2$$

der trinäre Teiler von $t^2 + cu^2$, in welchem N enthalten ist, und bezeichnet man mit k die Anzahl der ungeraden und ungleichen Primfaktoren, welche in c aufgehen, so besitzt Δ 2^{k-1} trinäre Formen, und diese sind von einander verschieden, da $N > c$ und umsomehr $N > \frac{2}{3}c$ ist (No. 287).

Dies vorausgeschickt, bestimmen die 2^{k-1} trinären Formen von N ebenso viele trinäre quadratische Teiler der Formel $t^2 + Nu^2$, in deren jedem c enthalten ist. Diese trinären Teiler sind sämtlich von einander verschieden, da sie unter einander verschiedenen trinären Werten von N entsprechen (No. 283); und da c nicht mehr wie 2^{k-1}-mal unter den quadratischen Teilern der Formel $t^2 + Nu^2$ ent-



halten sein kann (No. 245), so folgt daraus, dafs der gegebene Teiler Γ einer der 2^{k-1} trinären Teiler, welche c enthalten, sein mufs. Mithin ist Γ ein trinärer Teiler, und zwar besitzt dieser Teiler nur eine trinäre Form, was mit dem allgemeinen Satze übereinstimmt. Denn da in diesem Falle $i = 1$, so ergiebt sich $2^{i-1} = 1$.

306.

Mittelst dieses ersten Falles erkennt man, dafs, da die Tafel bis zur Grenze L als richtig erwiesen ist, die in dem allgemeinen Satze ausgesprochenen Eigenschaften noch bis zur Grenze $\frac{3}{4}L^2$ für alle Zahlen N bestehen bleiben, welche Primzahlen oder das Doppelte von Primzahlen und in der Formel $t^2 + Nu^2$ enthalten sind. Denn da $cy^2 + 2byz + az^2$ ein reciproker Teiler der Formel $t^2 + Nu^2$ ist, so kann man immer $c < 2\sqrt{\frac{1}{3}N}$ annehmen; somit ist $c < L$, wenn $N < \frac{3}{4}L^2$ ist.

307.

Ist jetzt N irgend eine Zahl, die unmittelbar über der Grenze L liegt, und ist $\Gamma = cy^2 + 2byz + az^2$ ein gegebener reciproker Teiler der Formel $t^2 + Nu^2$, so behaupte ich, dafs dieser Teiler 2^{i-1} trinäre Formen besitzt, wenn i die Anzahl der ungeraden und ungleichen Primfaktoren, welche in N aufgehen, bedeutet.

Es sei nämlich p eine Primzahl oder das Doppelte einer Primzahl, welche in dem Teiler Γ enthalten ist und zwischen den Grenzen $\frac{2}{3}L$ und $\frac{3}{4}L^2$ liegt. Diese Grenzen sind sehr weit von einander entfernt. Denn obwohl die Tafel nur bis zu $L = 251$ fortgesetzt ist, hat man $\frac{2}{3}L = 167$ und $\frac{3}{4}L^2 = 47251$. Alsdann ist die Zahl N ein Teiler von $t^2 + pu^2$, und als solcher enthalten in einem oder mehreren reciproken Teilern von $t^2 + pu^2$, welche man als bekannt und dem allgemeinen Gesetze gehorchend ansehen kann, weil p eine Primzahl oder das Doppelte einer Primzahl und kleiner als $\frac{3}{4}L^2$ ist. Da ferner die Zahl $N < \frac{3}{2}p$ ist, so kann sie nur einmal in jedem der quadratischen Teiler der Formel $t^2 + pu^2$ enthalten sein, und da sie nach der Anzahl ihrer Faktoren 2^{i-1}-mal in allen diesen Teilern enthalten sein mufs, so mufs es eine gleiche Anzahl, also 2^{i-1}, quadratische Teiler der Formel $t^2 + pu^2$ geben, von denen jeder einmal die Zahl N enthält.

Von diesen quadratischen Teilern, welche von einander verschieden sind, entspricht jeder einer verschiedenen trinären Form von p. Mithin giebt es 2^{i-1} von einander verschiedene trinäre Werte von p, deren jeder einer trinären Form von N entspricht. Und selbst wenn es unter diesen letzteren einander gleiche Formen gäbe (dies würde $p^2 = y^2 + Nz^2$ voraussetzen), so würde doch, weil diese gleichen trinären Formen von N ungleichen trinären Formen von p entsprechen, das System aus einer trinären Form von p und der entsprechenden trinären Form von N stets verschieden sein von jedem andern derartigen Systeme.

Dieselben Systeme, deren Anzahl 2^{i-1} ist, müssen auch entstehen, wenn man p als Teiler von $t^2 + Nu^2$ betrachtet (No. 285). Nun kann p, da es eine Primzahl oder das Doppelte einer Primzahl ist, nur zu einem einzigen quadratischen Teiler, welches der gegebene reciproke Teiler ist, gehören und in diesem nur auf eine einzige Art enthalten sein. Mithin ergiebt sich, da p in diesem Teiler 2^{i-1} verschiedene trinäre Formen annehmen mufs, dafs der Teiler Γ in 2^{i-1} trinäre Formen zerlegbar sein mufs, übereinstimmend mit dem Satze, welcher bewiesen werden sollte.

308.

Bemerkung. Der reciproke Teiler Γ, welcher zu der Formel $t^2 + Nu^2$, in welcher N durch i ungerade und ungleiche Primzahlen teilbar ist, gehört, kann nicht mehr als 2^{i-1} trinäre Formen haben. Denn ist, falls dies möglich wäre, die Anzahl seiner trinären Formen $= k > 2^{i-1}$, und ist P eine in dem Teiler Γ enthaltene Primzahl, welche gröfser ist als N^2, so besitzt die Zahl P als Teiler von $t^2 + Nu^2$ k trinäre Formen, welche einer gleichen Anzahl trinärer Formen von N entsprechen. Die k trinären Werte von P sind von einander verschieden, da man wegen $P > N^2$ der Gleichung

$$N^2 = y^2 + Pz^2$$

nicht genügen kann. Dies vorausgeschickt, bestimmen die k von einander verschiedenen trinären Werte von P eine gleiche Anzahl trinärer Teiler der Formel $t^2 + Pu^2$, in deren jedem N enthalten sein mufs. Mithin ist N $k$mal in den trinären Teilern von $t^2 + Pu^2$ enthalten. Da es aber nur i ungleiche Faktoren besitzt, so kann N nur 2^{i-1}-mal in den quadratischen Teilern von $t^2 + Pu^2$ enthalten sein. Mithin kann k nicht gröfser sein als 2^{i-1}.

Demnach ist die in dem allgemeinen Satze angegebene Zahl 2^{i-1}



die genaue Zahl der trinären Formen, welche der Teiler Γ annehmen kann und wirklich annimmt. Wenn jedoch N einen quadratischen Faktor hat, so kann es noch andere trinäre Formen des Teilers Γ geben; diese Formen würden indessen nur uneigentliche trinäre Formen sein, d. h. sie würden trinären Werten von c entsprechen, deren Glieder sämtlich durch dieselbe Quadratzahl teilbar wären. Diese Formen müssen aber, wie wir schon vorher bemerkt haben (No. 271), verworfen werden.

309.

Zweiter Beweis.

Um die Methode, auf welche dieser zweite Beweis sich gründet, klarer hervortreten zu lassen, wenden wir sie zunächst auf einige besondere Fälle an, indem wir der Reihe nach $c = 1, 2, 3, 5$ setzen und die entsprechenden Werte von b durch die Bedingung $b < \frac{1}{2}c$ oder $b = \frac{1}{2}c$ bestimmen. Lassen wir sodann a unbestimmt, so enthält jede Formel $cy^2 + 2byz + az^2$ unendlich viele andere, bei welchen der allgemeine Satz bestätigt ist.

Ist zunächst $c = 1$, so muſs $b = 0$ und $N = a$ sein, und der gegebene reciproke Teiler ist:

$$\Gamma = y^2 + az^2.$$

Da die Zahl 1 in diesem Teiler enthalten ist, so muſs N ein Teiler der Formel $t^2 + 1 \cdot u^2$ oder $t^2 + u^2$ sein, woraus folgt, daſs N oder $\frac{1}{2}N$ zu Primfaktoren nur Zahlen von der Form $4n + 1$ besitzen kann. Da nun die Anzahl dieser ungeraden und ungleichen Faktoren gleich i ist, so kann man der Gleichung $N = y^2 + z^2$ auf 2^{i-1} verschiedene Arten Genüge leisten.

Ist $N = f^2 + g^2$ eine von diesen Lösungen, so läſst sich Γ offenbar auf die trinäre Form

$$\Gamma = y^2 + f^2z^2 + g^2z^2$$

bringen, und dieser entspricht der trinäre Wert:

$$N = f^2 + g^2.$$

Da jede Zerlegung von N in zwei zu einander prime Quadrate ein ähnliches Resultat liefert, so nimmt offenbar der reciproke Teiler Γ 2^{i-1} trinäre Formen an, denen ebenso viele trinäre Werte von N entsprechen. Dies ist in Übereinstimmung mit dem allgemeinen Satze.

310.

Ist

$$c = 2,\ \Gamma = 2y^2 + 2byz + az^2,\ N = 2a - b^2,$$

so kann der Wert von b nur 0 oder 1 sein.

Da in beiden Fällen N ein Teiler von $t^2 + 2u^2$ sein mufs, so ist klar, dafs die Primfaktoren von N von derselben Form sind, und dafs man somit der Gleichung $N = y^2 + 2z^2$ auf 2^{i-1} verschiedene Arten genügen kann.

Stellt man eine dieser Lösungen durch $N = f^2 + 2g^2$ dar, so erhält man:

$$a = \frac{b^2 + f^2 + 2g^2}{2} = g^2 + \left(\frac{b+f}{2}\right)^2 + \left(\frac{b-f}{2}\right)^2.$$

Daraus erkennt man, dafs der Teiler Γ auf die trinäre Form

$$\Gamma = \left(y + \frac{b+f}{2}z\right)^2 + \left(y + \frac{b-f}{2}z\right)^2 + g^2z^2$$

gebracht werden kann. Derselben entspricht der trinäre Wert:

$$N = f^2 + g^2 + g^2.$$

Da nun N 2^{i-1}-mal von der Form $f^2 + 2g^2$ ist, so folgt hieraus, übereinstimmend mit dem allgemeinen Satze, dafs Γ 2^{i-1} trinäre Formen besitzt.

311.

Ist

$$c = 3,\ \Gamma = 3y^2 + 2byz + az^2,\ N = 3a - b^2,$$

so kann der Wert von b ebenfalls nur 0 oder 1 sein.

Da Γ ein reciproker Teiler und 3 in diesem Teiler enthalten ist, so mufs N ein Teiler der Formel $t^2 + 3u^2$ und als solcher in dem reciproken Teiler dieser Formel, nämlich in $2y^2 + 2yz + 2z^2$ enthalten sein. Es mufs demnach 2^{i-1} Lösungen der Gleichung

$$N = 2y^2 + 2yz + 2z^2$$

geben, falls N nicht teilbar ist durch 3, und nur 2^{i-2}, wenn N durch 3 sich teilen läfst.

Ist erstens $b = 0$ und $N = 3a$, und stellen wir einen der 2^{i-2} Werte von N durch $N = 2f^2 + 2fg + 2g^2$ dar, so erhalten wir:

$$a = \frac{2f^2 + 2fg + 2g^2}{3} = \frac{(2f+g)^2 + 3g^2}{2 \cdot 3}.$$

Aus diesem Werte erkennt man, dafs $2f + g$ durch 3 teilbar sein mufs. Ist also $2f + g = 3h$, so wird:

$$a = \frac{3h^2 + g^2}{2} = h^2 + \left(\frac{g+h}{2}\right)^2 + \left(\frac{g-h}{2}\right)^2.$$

Hieraus ergiebt sich folgende trinäre Form von Γ:

$$\Gamma = \left(y + \frac{g+h}{2}z\right)^2 + \left(y + \frac{h-g}{2}z\right)^2 + (y - hz)^2.$$

Da der Teiler $\Gamma = 3y^2 + az^2$ ambig ist, so erhält man eine zweite trinäre Form von Γ, indem man einfach das Zeichen von z ändert, also:

$$\Gamma = \left(y - \frac{g+h}{2} z\right)^2 + \left(y + \frac{g-h}{2} z\right)^2 + (y + hz)^2,$$

und der trinäre Wert von N, welcher diesen beiden Formen entspricht, ist:

$$N = f^2 + (f+g)^2 + g^2.$$

Da es nun 2^{i-2} ähnliche Werte von N giebt und jeder zwei trinäre Formen von Γ erzeugt, so ist offenbar die Gesamtzahl der trinären Formen von Γ gleich 2^{i-1}. Diesen entsprechen ebensoviele trinäre Formen von N, welche paarweise gleich sind.

Ist zweitens $b = 1$, $N = 3a - 1$, so besitzt N 2^{i-1} Werte von der Form $N = 2f^2 + 2fg + 2g^2$, von denen jeder ergiebt:

$$a = \frac{b^2 + 2f^2 + 2fg + 2g^2}{3} = \frac{2b^2 + (2f+g)^2 + 3g^2}{2 \cdot 3}.$$

Dieser Wert zeigt, dafs $2b^2 + (2f+g)^2$ durch 3 teilbar sein mufs; und da alsdann der Quotient nur von der Form $m^2 + 2n^2$ sein kann, so kann man setzen:

$$(2f+g)^2 + 2b^2 = 3(m^2 + 2n^2).$$

Dies giebt: $2f + g = m + 2n$, $b = m - n$, und daher:

$$a = \frac{m^2 + 2n^2 + g^2}{2} = \left(\frac{m+g}{2}\right)^2 + \left(\frac{m-g}{2}\right)^2 + n^2.$$

Da ferner $b = 1 = m - n$ ist, so kann man, wie ohne weiteres ersichtlich, den Teiler $\Gamma = 3y^2 + 2yz + az^2$ auf folgende Weise zerlegen:

$$\Gamma = \left(y + \frac{m+g}{2} z\right)^2 + \left(y + \frac{m-g}{2} z\right)^2 + (y - nz)^2.$$

Der entsprechende trinäre Wert von N ist:

$$N = g^2 + \left(\frac{m+g}{2} + n\right)^2 + \left(\frac{m-g}{2} + n\right)^2.$$

Dies kommt auf den Wert $N = g^2 + (f+g)^2 + f^2$ zurück.

Da man nun 2^{i-1} ähnliche Werte von N hat, so erhält man auch, in Übereinstimmung mit dem allgemeinen Satze, 2^{i-1} trinäre Formen des Teilers Γ.

312.

Ist $c = 5$ und der gegebene Teiler $\Gamma = 5y^2 + 2byz + az^2$, so ist $N = 5a - b^2$, und b kann nur einen der Werte 0, 1, 2 besitzen.

Welches auch dieser Wert sein möge, es mufs, da der Teiler Γ als reciprok vorausgesetzt und 5 darin enthalten ist, N ein Teiler von $t^2 + 5u^2$ und als solcher in den reciproken Teilern dieser Formel enthalten sein. Je nachdem aber N durch 5 teilbar ist oder nicht, sind zwei Fälle zu betrachten.

Ist zuerst $b = 0$ und $N = 5a$, so mufs, weil die Formel $t^2 + 5u^2$ nur den einen reciproken Teiler $y^2 + 5z^2$ hat, N 2^{i-2}-mal von der Form $y^2 + 5z^2$ sein. Bezeichnen wir einen dieser Werte mit

$$N = f^2 + 5g^2,$$

so erhalten wir:

$$\frac{f^2 + 5g^2}{5} = a.$$

Mithin mufs f durch 5 teilbar sein. Setzt man also $f = 5h$, so wird:

$$a = g^2 + 5h^2 = g^2 + h^2 + 4h^2.$$

Diese trinäre Form läfst die des Teilers Γ erkennen. Dieselbe ist:

$$\Gamma = (2y + hz)^2 + (y - 2hz)^2 + g^2z^2.$$

Beachtet man ferner, dafs der Teiler $5y^2 + az^2$ ambig ist, so erhält man durch Änderung des Zeichens von z die zweite trinäre Form:

$$\Gamma = (2y - hz)^2 + (y + 2hz)^2 + g^2z^2,$$

und diese beiden entsprechen demselben trinären Werte:

$$N = 25h^2 + 4g^2 + g^2.$$

Da die Anzahl der Lösungen der Gleichung $N = y^2 + 5z^2$ gleich 2^{i-2} ist und jede derselben zwei trinäre Formen von Γ liefert, so erhält man offenbar, in Übereinstimmung mit dem allgemeinen Satze, im Ganzen 2^{i-1} trinäre Formen von Γ.

Ist zweitens $b = 1$ oder 2 und $N = 5a - b^2$, so ist N, als Teiler von $t^2 + 5u^2$, 2^{i-1}-mal in dem quadratischen Teiler $y^2 + 5z^2$ enthalten.

Ist einer dieser Werte $N = f^2 + 5g^2$, so wird:

$$a = \frac{b^2 + f^2 + 5g^2}{5},$$

und dies zeigt, dafs $b^2 + f^2$ durch 5 teilbar sein mufs. Setzt man also $b^2 + f^2 = 5(m^2 + n^2)$, so erhält man hieraus $b = m - 2n$, $f = 2m + n$, und

$$a = m^2 + n^2 + g^2.$$

Dieser Wert von a und der von b lassen hinreichend deutlich die trinäre Form des Teilers Γ erkennen, nämlich:

$$\Gamma = (y + mz)^2 + (2y - nz)^2 + g^2 z^2.$$

Der entsprechende Wert von N ist:

$$N = (2m + n)^2 + g^2 + 4g^2,$$

und dieser kommt auf die gegebene Form $f^2 + g^2 + 4g^2$ zurück.

Da es nun 2^{i-1} solche Werte von N giebt, so giebt es auch 2^{i-1} trinäre Formen des Teilers Γ.

313.

Wir betrachten jetzt den reciproken Teiler

$$\Gamma = cy^2 + 2byz + az^2$$

in seiner ganzen Allgemeinheit und setzen nur voraus, dafs der Koefficient c prim zu N und kleiner als N sei, eine Bedingung, die jederzeit leicht zu erfüllen ist.*)

Hiernach mufs, da Γ ein reciproker Teiler ist, N ein Teiler der Formel $t^2 + cu^2$ und als solcher in den reciproken Teilern dieser Formel enthalten sein. Da ferner mit i die Anzahl der ungeraden und ungleichen Primfaktoren von N bezeichnet ist, so mufs N in den reciproken Teilern der Formel $t^2 + cu^2$ 2^{i-1}-mal vorkommen. Diese reciproken Teiler bilden eine von den Gruppen, in welche die Teiler dieser Formel zerfallen.

Ist daher $py^2 + 2qyz + rz^2$ einer von den reciproken Teilern der Formel $t^2 + cu^2$, in denen N enthalten ist, so kann man setzen:

$$N = pf^2 + 2qfg + rg^2 = ac - b^2,$$

und dies giebt:

$$a = \frac{b^2 + N}{c} = \frac{(pf + qg)^2 + cg^2 + pb^2}{cp}.$$

Aus diesem Ausdruck erkennt man, dafs $(pf + qg)^2 + cg^2$ durch c teilbar sein mufs. Um die Division auszuführen, nehmen wir an, dafs man alle quadratischen Teiler von $t^2 + pu^2$, welche c enthalten, gesucht habe. Irgend einer von diesen Teilern wird die Form

$$cy^2 + 2b'yz + a'z^2$$

besitzen, und die Werte von b' werden die sämtlichen Zahlen sein,

*) Siehe den IV. Hauptteil § 10. Diese Bedingung ist übrigens nicht absolut erforderlich für das Gelingen des Beweises, da man in den vorhergehenden Beispielen Fälle gesehen hat, in denen c und N einen gemeinsamen Teiler haben (No. 311 und 312). Anm. d. Verf.

die nicht gröſser als $\frac{c}{2}$ sind und der Gleichung $ca' - b'^2 = p$ genügen, oder für welche $b'^2 + p$ durch c teilbar wird.

Ist also

$$(pf + qg)^2 + pb^2 = cN',$$

so muſs sein:

$$N' = c\gamma^2 + 2b'\gamma\delta + a'\delta^2,$$

mithin:

$$cN' = (c\gamma + b'\delta)^2 + p\delta^2.$$

Da diese beiden Werte von cN' identisch sein müssen, so setze man:

$$\delta = b \quad \text{und} \quad c\gamma + b'\delta = \pm (pf + qg).$$

Dadurch ergiebt sich:

$$\gamma = \frac{\pm (pf + qg) - b'b}{c}.$$

Man hat daher unter den verschiedenen Werten von b' denjenigen zu suchen, für welchen γ eine ganze Zahl wird; einen solchen muſs man notwendigerweise finden, weil der gegebene Teiler Γ reciprok und dies die einzige Voraussetzung ist, auf welche sich diese Untersuchung stützt. Es kann auch nur einen solchen Wert von b' geben, für welchen γ eine ganze Zahl wird; denn gäbe es zwei b', β', so müſste $\frac{b'b \pm \beta'b}{c}$, oder, da c und b prim zu einander sind, $\frac{b' \pm \beta'}{c}$ eine ganze Zahl sein. Nun sind aber b' und β' alle beide kleiner als $\frac{1}{2}c$, oder falls eins von ihnen gleich $\frac{1}{2}c$ wäre, so müſste doch das andere kleiner als $\frac{1}{2}c$ sein, da sie von einander verschieden sind. Mithin ist die Summe $b' + \beta'$ kleiner als c, sie kann daher nicht durch c teilbar sein. Man muſs auch beachten, daſs die Zahlen γ und δ oder γ und b gerade die Zahlen sind, welche die Rechnung ergiebt, und demnach zufälligerweise einen gemeinschaftlichen Teiler haben können, denn gegenwärtig wird nichts anderes gesucht als die Form der bestimmten Zahl N'. Nachdem aber γ gefunden ist, hat man:

$$N' = c\gamma^2 + 2b'\gamma\delta + a'\delta^2.$$

Da nun der quadratische Teiler $cy^2 + 2b'yz + a'z^2$ der Formel $t^2 + pu^2$ auf die Form $p'y^2 + 2q'yz + r'z^2$, in welcher $p' < 2\sqrt{\frac{1}{3}p}$ ist, gebracht werden kann, so nimmt der Wert von N' die Form an:

$$N' = p'f'^2 + 2q'f'g' + r'g'^2,$$

in welcher f' und g' je nach den verschiedenen Fällen einen gemeinschaftlichen Teiler haben können oder nicht.



Nachdem dieses festgestellt ist, wird der Wert von a:

$$a = \frac{g^2 + N'}{p} = \frac{(p'f' + q'g')^2 + pg'^2 + p'g^2}{pp'},$$

und aus diesem neuen Ausdruck sieht man, dafs $(p'f' + q'g')^2 + p'g^2$ durch p teilbar sein mufs. Setzt man also:

$$(p'f' + q'g')^2 + p'g^2 = pN'',$$

so findet man durch ähnliche Rechnungen, wie vorher:

$$N'' = p''f''^2 + 2q''f''g'' + r''g''^2,$$

einen Ausdruck, in welchem man $p'' < 2\sqrt{\frac{1}{3}p'}$ voraussetzen darf. Man erhält daher folgenden dritten Wert von a:

$$a = \frac{g'^2 + N''}{p'} = \frac{(p''f'' + q''g'')^2 + p'g''^2 + p''g'^2}{p'p''}.$$

Diese verschiedenen Rechnungen müssen so lange fortgesetzt werden, bis die beiden letzten Glieder der abnehmenden Reihe $p, p', p'', \ldots$ 1 und 1 oder 2 und 1 sind. Wenn alle beide gleich der Einheit sind, so ist der letzte Wert von a von der Form:

$$\lambda^2 + \mu^2 + \nu^2;$$

ist aber das letzte Glied 1 und das vorletzte 2, so wird a von der Form $\frac{\lambda^2 + \mu^2 + 2\nu^2}{2}$, welche sich ebenfalls in eine Summe von drei Quadraten verwandelt, nämlich in

$$\nu^2 + \left(\frac{\lambda + \mu}{2}\right)^2 + \left(\frac{\lambda - \mu}{2}\right)^2.$$

Allgemein ist also stets die Zahl a auf eine trinäre Form von der Art wie $\lambda^2 + \mu^2 + \nu^2$ zurückgeführt. Zu gleicher Zeit findet man im Verlaufe der Rechnungen, dafs b auf die Form gebracht werden kann:

$$b = \lambda l + \mu m + \nu n,$$

und hieraus folgt, dafs der gegebene Teiler Γ sich in folgender Weise in drei Quadrate zerlegen läfst:

$$\Gamma = (ly + \lambda z)^2 + (my + \mu z)^2 + (ny + \nu z)^2.$$

Man kann aber zu diesem Resultat noch weit unmittelbarer, und ohne den vorstehenden Wert von b zu Hülfe zu nehmen, gelangen.

314.

Man kann nämlich die zur Bestimmung des trinären Wertes von a erforderlichen Rechnungen ausführen, wenn a und b unbestimmt bleiben, da die Zahlen $p, p', \ldots$, auf denen diese Rechnungen beruhen, aus der einen bekannten Zahl c entstehen, so dafs sie stets

dieselben bleiben oder nur eine Änderung erleiden durch die Wahl, welche man unter den Werten von p' treffen kann, wenn es mehrere die Zahl c enthaltende quadratische Teiler von $t^2 + pu^2$ giebt, oder unter den Werten von p'', wenn es mehrere die Zahl p enthaltende quadratische Teiler von $t^2 + p'u^2$ giebt, u. s. f. In allen Fällen ist die Reihe $p, p', p'', \ldots$ stets so beschaffen, dafs

$$p' < \sqrt{\tfrac{4}{3}p}, \; p'' < \sqrt{\tfrac{4}{3}p'}, \ldots$$

ist, so dafs diese Reihe sehr schnell bis zum letzten Gliede 1 abnimmt. Man kann also auf diese Weise zu allgemeinen Resultaten gelangen, welche auf unendlich viele Werte von N anwendbar sind, wie wir dies in den Beispielen für den Fall $c = 1, 2, 3, 5$ gesehen haben.

Wenn man aber auch N als bestimmt gegeben ansieht, so kann man doch in den gegebenen Teiler eine Unbestimmte einführen, vermöge deren seine Zerlegung in drei Quadrate bedeutend erleichtert wird. Zu diesem Zwecke braucht man nur $y + kz$ an die Stelle von y zu setzen, wodurch der Teiler Γ übergeht in:

$$\Gamma = cy^2 + 2(b + ck)yz + (a + 2bk + ck^2)z^2.$$

Wendet man die vorige Methode auf diesen Teiler an, so sind die Zahlen $p, p', p'', \ldots$, ohne irgendwelche Veränderung, dieselben, als ob $k = 0$ wäre. Man erhält daher auch den Wert des letzten Koefficienten $a + 2bk + ck^2$ ausgedrückt durch drei Quadrate, und diese Quadrate, in denen k unbestimmt bleibt, können nur von der Form sein:

$$(l + \lambda k)^2 + (m + \mu k)^2 + (n + \nu k)^2,$$

woraus unmittelbar die trinäre Form von Γ sich ergiebt:

$$\Gamma = (ly + \lambda z)^2 + (my + \mu z)^2 + (ny + \nu z)^2.$$

Durch dieses Hülfsmittel vermeidet man jedes Probieren bei der Bestimmung des trinären Wertes von Γ und gelangt zu diesem zu gleicher Zeit auf die einfachste und direkteste Weise. Da nun die Zahl N auf 2^{i-1} verschiedene Arten in den quadratischen Teilern der Formel $t^2 + cu^2$ enthalten ist, so ergiebt jeder dieser Ausdrücke eine trinäre Form des Teilers Γ; mithin besitzt dieser Teiler, in Übereinstimmung mit dem allgemeinen Satze, 2^{i-1} trinäre Formen.

Durch diese Analyse kann die Grenze der Tafel VIII, welche zunächst beliebig ist, unendlich weit hinausgerückt werden; der angeführte Satz wird in ihrer ganzen Ausdehnung gelten.



315.

Beispiel.

Es sei der reciproke Teiler

$$\Gamma = 189y^2 + 30yz + 50z^2$$

gegeben, welcher zur Formel $t^2 + Nu^2$, in der $N = 9225 = 3^2 \cdot 5^2 \cdot 41$ ist, gehört. Es handelt sich darum zu zeigen, dafs dieser Teiler auf 2^{3-1} oder 4 Arten in drei Quadrate zerlegt werden kann.

Da die äufseren Koefficienten 50 und 189 beide mit N einen gemeinschaftlichen Teiler haben, so haben wir, um nach der allgemeinen Methode verfahren zu können, in Γ eine Zahl zu suchen, welche prim zu N ist. Diese Zahl erhält man unmittelbar, wenn man $y = 1$ und $z = -1$ setzt, wodurch sich das Resultat ergiebt: $189 - 30 + 50 = 209 = 11 \,.\, 19$, also eine Zahl, welche mit N keinen gemeinschaftlichen Teiler hat. Man mufs daher zuvörderst bewirken, dafs 209 der erste Koefficient von Γ wird. Dazu reicht es hin, $z - y$ an Stelle von z zu setzen, und sodann das Vorzeichen von z zu ändern. Auf diese Weise ergiebt sich:

$$\Gamma = 209y^2 + 70yz + 50z^2.$$

Setzt man endlich $y + kz$ an Stelle von y, um in den letzten Koefficienten eine Unbestimmtheit einzuführen, so erhält man:

$$\Gamma = 209y^2 + 2(35 + 209k)yz + (50 + 70k + 209k^2)z^2.$$

Wir setzen also:

$$c = 209, \quad b = 35 + 209k, \quad a = 50 + 70k + 209k^2.$$

Die Zahl N, welche drei ungleiche Primfaktoren besitzt, mufs 2^{3-1} oder 4-mal in den reciproken Teilern von $t^2 + 209u^2$ enthalten sein. Nun besitzt aber diese Formel drei reciproke Teiler, nämlich:

$$\begin{aligned} 2y^2 &+ 2yz + 105z^2 \\ 10y^2 &+ 2yz + 21z^2 \\ 13y^2 &+ 10yz + 18z^2, \end{aligned}$$

und in der That findet man, dafs 9225 einmal in dem zweiten und dreimal in dem dritten von diesen Teilern enthalten ist, und zwar auf folgende Weise:

$$N = 10f^2 + 2fg + 21g^2 \quad \begin{cases} f = 29 \\ g = 5 \end{cases}$$

$$N = 13f^2 + 10fg + 18g^2 \quad \begin{cases} f = 27, \quad 27, \quad 19 \\ g = -1, \; -14, \; -22. \end{cases}$$

Betrachten wir zunächst die dritte Form, welche drei trinäre Werte von Γ liefern mufs, so erhält man mittelst dieser Form:

$$a = \frac{b^2 + N}{c} = \frac{13b^2 + (13f + 5g)^2 + 209g^2}{209 \,.\, 13}.$$

Die erste Rechnung besteht darin, dafs man den Quotienten sucht, welcher sich bei der Division von $(13f + 5g)^2 + 13b^2$ durch 209 ergiebt. Nun mufs 209, weil es zwei Faktoren 11 und 19 hat, zweimal in den quadratischen Teilern von $t^2 + 13u^2$ enthalten sein, und in der That ist, wenn der quadratische Teiler, welcher 209 enthält, durch

$$209y^2 + 2b'yz + a'z^2$$

dargestellt wird, die Bedingung $209a' - b'^2 = 13$ auf zweierlei Weise erfüllt, einmal wenn man $b' = 14$, $a' = 1$, das andere Mal, wenn man $b' = 52$, $a' = 13$ setzt. Man kann daher

$$\frac{(13f + 5g)^2 + 13b^2}{209} = 209y^2 + 2b'yz + a'z^2$$

setzen, und dies giebt:

$$(13f + 5g)^2 + 13b^2 = (209y + b'z)^2 + 13z^2.$$

Folglich ist:

$$z = b \quad \text{und} \quad 209y + b'z = \pm (13f + 5g),$$

also:

$$y = \frac{\pm (13f + 5g) - b'b}{209}.$$

Nehmen wir für f und g die Lösung $f = 19$, $g = -32$, so ist $13f + 5g = 137$ und:

$$y = \frac{\pm 137 - b'(35 + 209k)}{209}.$$

In diesem Ausdrucke mufs man das Zeichen von 137 und den Wert von b' derart wählen, dafs y eine ganze Zahl ist. Man erreicht dies, wenn das untere Zeichen genommen und $b' = 14$ gesetzt wird. Es ist daher:

$$y = -3 - 14k.$$

Der gesuchte Quotient ist $209y^2 + 28yz + z^2$ und seine einfachste Form: $(z + 14y)^2 + 13y^2$. Stellt man diese durch $f'^2 + 13g'^2$ dar, so hat man also:

$$f' = -7 + 13k$$
$$g' = -3 - 14k,$$

und der Wert von a wird:

$$a = \frac{g^2 + f'^2 + 13g'^2}{13}.$$

Es ist daher nur noch $g^2 + f'^2$ durch 13 zu dividieren. Dazu mufs man 13 als Teiler der Formel $t^2 + u^2$ betrachten. Diese Formel be-



sitzt aber nur einen quadratischen Teiler $y^2 + z^2$, und dieser geht, wenn man denselben so umgestaltet, dafs 13 der erste Koefficient desselben wird, über in:

$$13y^2 + 10yz + 2z^2.$$

Ist daher:

$$g^2 + f'^2 = 13(13y^2 + 10yz + 2z^2) = (13y + 5z)^2 + z^2,$$

so kann man setzen:

$$z = g \quad \text{und} \quad 13y + 5z = \pm f',$$

oder:

$$z = f' \quad \text{und} \quad 13y + 5z = \pm g.$$

Aus diesen beiden Lösungen ergiebt sich aber in gleicher Weise, dafs sich die Gröfse

$$\frac{g^2 + f'^2}{13} = 13y^2 + 10yz + 2z^2 = (z + 2y)^2 + (z + 3y)^2$$

auf

$$(4 + 2k)^2 + (5 - 3k)^2$$

reduciert. Mithin hat man:

$$a = (14k + 3)^2 + (2k + 4)^2 + (3k - 5)^2,$$

und da dies der Wert von $50 + 70k + 209k^2$ ist, so folgt, dafs der Teiler $\Gamma = 209y^2 + 70yz + 50z^2$ die trinäre Form besitzt:

$$(14y + 3z)^2 + (2y + 4z)^2 + (3y - 5z)^2.$$

Setzt man $z - y$ für z und ändert man sodann das Zeichen von z, so nimmt der Teiler Γ wieder die ursprünglich gegebene Form $189y^2 + 30yz + 50z^2$ an, und die soeben gefundene trinäre Form geht über in:

$$(11y - 3z)^2 + (2y + 4z)^2 + (8y + 5z)^2.$$

Sucht man in derselben Weise die beiden andern trinären Formen, welche aus der Form $N = 13f^2 + 10fg + 18g^2$ entstehen, und ebenso die, welche aus der Form $N = 10f^2 + 2fg + 21g^2$ entspringt, so erhält man die vier trinären Formen des gegebenen Teilers $\Gamma = 189y^2 + 30yz + 50z^2$. Diese vier trinären Formen und die entsprechenden trinären Werte von N sind:

$\Gamma = (11y - 3z)^2 + (2y + 4z)^2 + (8y + 5z)^2$	$N = 79^2 + 50^2 + 22^2$
$\Gamma = (10y - 4z)^2 + (8y + 5z)^2 + (5y + 3z^2)$	$N = 82^2 + 50^2 + 1^2$
$\Gamma = (13y - z)^2 + (2y)^2 + (4y + 7z)^2$	$N = 95^2 + 14^2 + 2^2$
$\Gamma = (10y + 4z)^2 + (8y - 5z)^2 + (5y + 3z)^2$	$N = 82^2 + 49^2 + 10^2$

316.

Allgemeine Folgerungen.

Das Ergebnis dieser Theorie, welches zum gröfsten Teile in der Tafel VIII niedergelegt ist, besteht in folgenden Eigenschaften, die jetzt mit aller erforderlichen Allgemeinheit als bewiesen anzusehen sind:

1) Jede Formel $t^2 + cu^2$, in welcher c weder von der Form $4n$ noch von der Form $8n + 7$ ist, enthält stets wenigstens einen reciproken quadratischen, d. h. einen quadratischen Teiler von der Beschaffenheit, dafs, wenn N irgend eine in diesem Teiler enthaltene Zahl bedeutet, die Zahl c ein Teiler der Formel $t^2 + Nu^2$ ist.

2) Jeder reciproke quadratische Teiler ist zugleich trinär, d. h. er läfst sich ganz allgemein in drei Quadrate zerlegen, ohne dafs man den in ihm enthaltenen unbestimmten Gröfsen bestimmte Werte beilegt.

3) Im Falle c von der Form $8n + 3$ ist, enthält der reciproke Teiler nur Zahlen von der Form $4n + 2$, und er wird dargestellt durch die Formel $2py^2 + 2qyz + 2rz^2$, in welcher $4pr - q^2 = c$ ist.

4) Ist c oder $\frac{1}{2}c$ eine Primzahl oder allgemein eine Potenz einer Primzahl, so läfst sich jeder reciproke Teiler der Formel $t^2 + cu^2$ nur auf eine einzige Weise in drei Quadrate zerlegen; er besitzt somit nur eine trinäre Form.

5) Ist dagegen c oder $\frac{1}{2}c$ durch i verschiedene Primzahlen teilbar, so besitzt jeder reciproke Teiler der Formel $t^2 + cu^2$ 2^{i-1} trinäre Formen.

6) Jeder trinäre Teiler ist notwendig reciprok, und jeder reciproke Teiler ist zu gleicher Zeit trinär. Diese beiden Eigenschaften sind untrennbar mit einander verbunden und gehören ausschliefslich einer der Gruppen an, in welche die quadratischen Teiler einer und derselben Formel $t^2 + cu^2$ zerfallen (No. 204 u. 205).

7) Ist c eine Primzahl von der Form $4n + 1$ oder das Doppelte einer beliebigen Primzahl, so ist jeder quadratische Teiler der Formel $t^2 + cu^2$, welcher die Form $4n + 1$ besitzt, ein reciproker Teiler.

8) Ist c eine Primzahl von der Form $8n + 3$, so ist



jeder quadratische Teiler der Formel $t^2 + cu^2$, welcher die Form $4n + 2$ besitzt, ein reciproker Teiler.

9) Jede trinäre Form eines reciproken Teilers entspricht stets einer trinären Form der Zahl c, so dafs es für jeden reciproken Teiler ebensoviel trinäre Formen der Zahl c giebt, als trinäre Formen dieses Teilers vorhanden sind.

10) Die aus demselben reciproken Teiler abgeleiteten trinären Werte der Zahl c sind paarweise gleich, wenn dieser Teiler ambig ist (den Teiler $py^2 + 2qyz + rz^2$ nennen wir ambig, wenn er zu einem der drei Fälle $q = 0$, $2q = p$ oder $= r$, $p = r$ gehört, und wenn zugleich der kleinere der beiden Koefficienten p und r gröfser als 2 ist).

11) In jedem andern Falle sind die aus demselben trinären oder reciproken Teiler abgeleiteten trinären Werte von c von einander verschieden; sie sind es stets, wenn sie aus zwei verschiedenen reciproken Teilern abgeleitet sind.

12) Die in jedem trinären oder reciproken Teiler enthaltenen Zahlen gehören stets, ebenso wie die Zahlen c, zu einer der Formen $4n + 1$, $4n + 2$, $8n + 3$. Es kann in ihnen keine Zahl von der Form $4n$ oder $8n + 7$ vorkommen.

13) Ist N in einem reciproken Teiler der Formel $t^2 + cu^2$, und somit c in einem reciproken Teiler der Formel $t^2 + Nu^2$ enthalten, so sind die entsprechenden trinären Werte von N und c in beiden Fällen dieselben.

317.

Satz 13. Jede ungerade Zahl, mit alleiniger Ausnahme der Zahlen von der Form $8n + 7$, ist die Summe von drei Quadraten.

Dieser Satz ist eine sehr einfache Folgerung aus der vorstehenden Theorie. Denn jede ungerade Zahl c, welche nicht von der Form $8n + 7$ ist, ist entweder von der Form $4n + 1$ oder von der Form $8n + 3$. Mithin ist die Formel $t^2 + cu^2$ unter denen auf Tafel VIII, welche man als unbegrenzt betrachten mufs, enthalten. Durch den Satz 10 wird aber gezeigt, dafs jede Formel dieser Tafel wenigstens einen reciproken quadratischen Teiler hat, und durch

Satz 12 wird bewiesen, dafs dieser Teiler trinär ist, und dafs es somit wenigstens einen entsprechenden trinären Wert von c giebt. Mithin ist jede ungerade Zahl von der Form $4n+1$ und $8n+3$ die Summe dreier Quadrate.

318.

Zugleich folgt aus der vorstehenden Theorie, dafs auch, wenn c selbst quadratische Faktoren hätte, c immer als Summe von drei Quadraten, welche keinen gemeinschaftlichen Teiler haben, dargestellt werden könnte; denn wir betrachten als trinäre Formen stets nur diejenigen, welche dieser Bedingung genügen. Die Tafel VIII enthält keine andern.

So hat man z. B.

$$81 = 8^2 + 4^2 + 1,\ 225 = 14^2 + 5^2 + 2^2,\ \text{u. s. w.}$$

Hieraus ersieht man, dafs jede Zahl von der Form $4n+1$ oder $8n+3$ wenigstens eine trinäre Form besitzt, welche ihr eigentümlich und von denen der niedrigeren Zahlen unabhängig ist.

Der Teil dieses Satzes, welcher sich auf die Zahlen von der Form $8n+3$ bezieht, beweist, dafs jede ganze Zahl die Summe dreier Trigonalzahlen ist. Dies ist der berühmte Fermatsche Satz, dessen wir in No. 155 Erwähnung gethan haben.

319.

Satz 14. Jede Zahl, welche das Doppelte einer ungeraden Zahl ist, ist die Summe dreier Quadrate.

Es ist dies ebenfalls eine unmittelbare Folge der Sätze 10 und 12, wenn man dieselben auf die Tafel VIII anwendet; überdies erkennt man mit Hülfe dieser Theorie, dafs die in Rede stehende Zahl von der Form $4n+2$ stets in drei Quadrate zerlegt werden kann, welche keinen gemeinschaftlichen Teiler haben.

320.

Zusatz 1. Wird irgend eine Zahl, welche das Doppelte einer ungeraden Zahl ist, mit $4a+2$ bezeichnet, so kann man stets der Gleichung

$$4a + 2 = x^2 + y^2 + z^2$$

Genüge leisten. Aus der Form der linken Seite erkennt man aber, dafs von diesen drei Quadraten x^2, y^2, z^2 zwei ungerade und eins

gerade sein mufs. Setzt man daher $x = p + q$, $y = p - q$, $z = 2r$, so erhält man:

$$2a + 1 = p^2 + q^2 + 2r^2.$$

Mithin ist jede ungerade Zahl von der Form $p^2 + q^2 + 2r^2$.

Von diesem Satze hatte Fermat behauptet, dafs er den Primzahlen von der Form $8n + 7$ eigentümlich sei. Wie man sieht, kommt derselbe aber allen ungeraden Zahlen zu, und man wird ferner stets bemerken, dafs, selbst wenn die betreffende Zahl durch eine Quadratzahl teilbar wäre, man doch immer voraussetzen darf, dafs die drei Quadrate p^2, q^2, r^2 keinen gemeinschaftlichen Teiler haben.

321.

Zusatz 2. Eine beliebige ganze Zahl läfst sich stets durch eine der Formeln $(2a + 1)2^{2n}$, $(2a + 1)2^{2n+1}$ darstellen. Gehört dieselbe zur ersten Form, so ist sie, nach dem soeben bewiesenen Satze, von der Form $2^{2n}(p^2 + q^2 + 2r^2)$; gehört sie zur zweiten, so ist sie von der Form $2^{2n}(p^2 + q^2 + r^2)$. Mithin:

Jede ganze Zahl, oder wenigstens das Doppelte derselben, ist die Summe von drei Quadraten.

322.

Satz 15. Ist N eine beliebige Zahl von einer der Formen $4n + 1$, $4n + 2$, $8n + 3$, welche alle ungeraden Zahlen oder das Doppelte derselben mit alleiniger Ausnahme der Zahlen von der Form $8n + 7$ umfassen, und bezeichnet man mit i die Anzahl der ungeraden und ungleichen Primfaktoren, welche in N aufgehen, so ist die Anzahl der trinären Formen von N stets gleich einem Vielfachen von 2^{i-2} und daher nicht kleiner als 2^{i-2}.

Es sei nämlich $m + n$ die Anzahl der reciproken Teiler von $t^2 + Nu^2$, und zwar gebe es unter diesen m ambige und n nicht ambige. Jeder nicht ambige reciproke Teiler kann in 2^{i-1} trinäre Formen zerlegt werden, denen eine gleiche Anzahl von einander verschiedener trinärer Formen von N entspricht. Jeder ambige Teiler kann ebenso in 2^{i-1} trinäre Formen zerlegt werden; da jedoch je zwei von diesen gleichen trinären Werten von N entsprechen, so ist die Anzahl der letzteren nur gleich 2^{i-2}. Wird daher die Gesamtzahl der trinären Werte von N mit x bezeichnet, so erhält man:

$$x = 2^{i-2}(2n + m).$$

Mithin ist diese Anzahl niemals kleiner als 2^{i-2} und im Allgemeinen ein Vielfaches von 2^{i-2}. Ist $i = 1$, so reduciert sich die Formel auf $x = n$, da es in diesem Falle keinen ambigen Teiler geben kann.

Wendet man diesen Satz auf die Zahl $9225 = 3^2 \cdot 5^2 \cdot 41$ an und beachtet man, dafs die Formel $t^2 + 9225u^2$ fünf reciproke Teiler hat, von denen zwei ambig sind, so hat man $m = 2$, $n = 3$, $i = 3$. Mithin ist die Anzahl der trinären Formen von N gleich

$$2(6 + 2) = 16,$$

und dies wird durch die folgende Tafel bestätigt:

$95^2 + 14^2 + 2^2$	$85^2 + 44^2 + 8^2$	$80^2 + 53^2 + 4^2$	$70^2 + 58^2 + 31^2$
$94^2 + 17^2 + 10^2$	$83^2 + 44^2 + 20^2$	$80^2 + 52^2 + 11^2$	$70^2 + 47^2 + 46^2$
$92^2 + 20^2 + 19^2$	$82^2 + 50^2 + 1^2$	$79^2 + 50^2 + 22^2$	$67^2 + 56^2 + 40^2$
$88^2 + 35^2 + 16^2$	$82^2 + 49^2 + 10^2$	$76^2 + 43^2 + 40^2$	$65^2 + 62^2 + 34^2$.

323.

Hieraus kann man ein ziemlich leichtes **Verfahren** zur Ermittlung einer Zahl, welche beliebig viele trinäre Formen besitzt, ableiten. Soll diese Zahl nicht weniger als eine gegebene Anzahl von trinären Formen besitzen, so braucht man nur eine gewisse Anzahl von ungleichen Primfaktoren mit einander zu multiplicieren. Soll z. B. eine Zahl wenigstens 32 trinäre Formen besitzen, so wird diese Zahl, wenn man sie aus sieben Faktoren zusammensetzt, sicher der Aufgabe genügen, wofern sie nicht von der Form $8n + 7$ ist. Eine solche Zahl ist z. B.: $3 . 5 . 7 . 11 . 13 . 17 . 19$, und diese ist von der Form $8n + 5$.

Will man aber, dafs die gesuchte Zahl genau eine bestimmte Anzahl von trinären Formen besitze, so bedarf es, um zu diesem Ziele zu gelangen, einiger Versuche. Soll z. B. $x = 20$ sein, so kann man $i = 4$ und $2n + m = 5$ setzen; alsdann hat man nur noch unter den einfachsten, aus vier ungleichen Primfaktoren zusammengesetzten Zahlen, welche nicht von der Form $8n + 7$ sind, diejenige zu bestimmen, welche entweder drei reciproke Teiler, von denen einer ambig ist, oder vier reciproke Teiler, von denen drei ambig sind, besitzt. In diesen beiden Fällen ist nämlich in gleicher Weise:

$$2n + m = 5.$$



Tafel I.

Die einfachsten Ausdrücke der Formeln $Ly^2 + 2Myz + Nz^2$ für alle Werte der nichtquadratischen Zahl $A = M^2 - LN$ von $A = 2$ bis $A = 136$.

Zahl A.	Reducierte Formel.	Zahl A.	Reducierte Formel.
2	$y^2 - 2z^2$	31	$\pm(y^2 - 31z^2)$
3	$\pm(y^2 - 3z^2)$	32	$\pm(y^2 - 32z^2)$
5	$y^2 - 5z^2$	33	$\pm(y^2 - 33z^2)$
6	$\pm(y^2 - 6z^2)$	34	$\pm(y^2 - 34z^2)$
7	$\pm(y^2 - 7z^2)$		$\pm(3y^2 + 2yz - 11z^2)$
8	$\pm(y^2 - 8z^2)$	35	$\pm(y^2 - 35z^2)$
10	$y^2 - 10z^2$		$\pm(5y^2 - 7z^2)$
	$2y^2 - 5z^2$	37	$y^2 - 37z^2$
11	$\pm(y^2 - 11z^2)$		$3y^2 + 2yz - 12z^2$
12	$\pm(y^2 - 12z^2)$	38	$\pm(y^2 - 38z^2)$
13	$y^2 - 13z^2$	39	$\pm(y^2 - 39z^2)$
14	$\pm(y^2 - 14z^2)$		$\pm(2y^2 + 2yz - 19z^2)$
15	$\pm(y^2 - 15z^2)$	40	$\pm(y^2 - 40z^2)$
	$\pm(3y^2 - 5z^2)$		$\pm(5y^2 - 8z^2)$
17	$y^2 - 17z^2$	41	$y^2 - 41z^2$
18	$\pm(y^2 - 18z^2)$	42	$\pm(y^2 - 42z^2)$
19	$\pm(y^2 - 19z^2)$		$\pm(2y^2 - 21z^2)$
20	$\pm(y^2 - 20z^2)$	43	$\pm(y^2 - 43z^2)$
21	$\pm(y^2 - 21z^2)$	44	$\pm(y^2 - 44z^2)$
22	$\pm(y^2 - 22z^2)$	45	$\pm(y^2 - 45z^2)$
23	$\pm(y^2 - 23z^2)$	46	$\pm(y^2 - 46z^2)$
24	$\pm(y^2 - 24z^2)$	47	$\pm(y^2 - 47z^2)$
	$\pm(3y^2 - 8z^2)$	48	$\pm(y^2 - 48z^2)$
26	$y^2 - 26z^2$		$\pm(3y^2 - 16z^2)$
	$2y^2 - 13z^2$	50	$y^2 - 50z^2$
27	$\pm(y^2 - 27z^2)$		$2y^2 - 25z^2$
28	$\pm(y^2 - 28z^2)$	51	$\pm(y^2 - 51z^2)$
29	$y^2 - 29z^2$		$\pm(3y^2 - 17z^2)$
30	$\pm(y^2 - 30z^2)$		
	$\pm(2y^2 - 15z^2)$		

Zahl A.	Reducierte Formel.
52 53 54	$\pm(y^2 - 52z^2)$ $y^2 - 53z^2$ $\pm(y^2 - 54z^2)$
55	$\pm(y^2 - 55z^2)$ $\pm(2y^2 + 2yz - 27z^2)$
56	$\pm(y^2 - 56z^2)$ $\pm(5y^2 + 2yz - 11z^2)$
57	$\pm(y^2 - 57z^2)$
58	$y^2 - 58z^2$ $2y^2 - 29z^2$
59	$\pm(y^2 - 59z^2)$
60	$\pm(y^2 - 60z^2)$ $\pm(3y^2 - 20z^2)$
61 62	$y^2 - 61z^2$ $\pm(y^2 - 62z^2)$
63	$\pm(y^2 - 63z^2)$ $\pm(7y^2 - 9z^2)$
65	$y^2 - 65z^2$ $5y^2 - 13z^2$
66	$\pm(y^2 - 66z^2)$ $\pm(3y^2 - 22z^2)$
67 68 69	$\pm(y^2 - 67z^2)$ $\pm(y^2 - 68z^2)$ $\pm(y^2 - 69z^2)$
70	$\pm(y^2 - 70z^2)$ $\pm(2y^2 - 35z^2)$
71	$\pm(y^2 - 71z^2)$
72	$\pm(y^2 - 72z^2)$ $\pm(4y^2 + 4yz - 17z^2)$
73	$y^2 - 73z^2$
74	$y^2 - 74z^2$ $2y^2 - 37z^2$
75	$\pm(y^2 - 75z^2)$ $\pm(3y^2 - 25z^2)$
76 77	$\pm(y^2 - 76z^2)$ $\pm(y^2 - 77z^2)$
78	$\pm(y^2 - 78z^2)$ $\pm(2y^2 - 39z^2)$
79	$\pm(y^2 - 79z^2)$ $\pm(3y^2 + 2yz - 26z^2)$
80	$\pm(y^2 - 80z^2)$ $\pm(5y^2 - 16z^2)$
82	$y^2 - 82z^2$ $2y^2 - 41z^2$ $3y^2 + 2yz - 27z^2$
83	$\pm(y^2 - 83z^2)$
84	$\pm(y^2 - 84z^2)$ $\pm(7y^2 - 12z^2)$
85	$y^2 - 85z^2$ $3y^2 + 2yz - 28z^2$
86	$\pm(y^2 - 86z^2)$
87	$\pm(y^2 - 87z^2)$ $\pm(3y^2 - 29z^2)$
88	$\pm(y^2 - 88z^2)$ $\pm(8y^2 - 11z^2)$
89	$y^2 - 89z^2$
90	$\pm(y^2 - 90z^2)$ $\pm(2y^2 - 45z^2)$
91	$\pm(y^2 - 91z^2)$ $\pm(7y^2 - 13z^2)$
92 93 94	$\pm(y^2 - 92z^2)$ $\pm(y^2 - 93z^2)$ $\pm(y^2 - 94z^2)$
95	$\pm(y^2 - 95z^2)$ $\pm(2y^2 + 2yz - 47z^2)$

Zahl A.	Reducierte Formel.	Zahl A.	Reducierte Formel.
96	$\pm(y^2 - 96z^2)$ $\pm(3y^2 - 32z^2)$	116 117 118	$\pm(y^2 - 116z^2)$ $\pm(y^2 - 117z^2)$ $\pm(y^2 - 118z^2)$
97 98	$y^2 - 97z^2$ $\pm(y^2 - 98z^2)$	119	$\pm(y^2 - 119z^2)$ $\pm(7y^2 - 17z^2)$
99	$\pm(y^2 - 99z^2)$ $\pm(9y^2 - 11z^2)$ $\pm(7y^2 + 2yz - 14z^2)$	120	$\pm(y^2 - 120z^2)$ $\pm(3y^2 - 40z^2)$ $\pm(5y^2 - 24z^2)$ $\pm(15y^2 - 8z^2)$
101	$y^2 - 101z^2$ $4y^2 + 2yz - 25z^2$		
102	$\pm(y^2 - 102z^2)$ $\pm(3y^2 - 34z^2)$	122	$y^2 - 122z^2$ $2y^2 - 61z^2$
103	$\pm(y^2 - 103z^2)$	123	$\pm(y^2 - 123z^2)$ $\pm(3y^2 - 41z^2)$
104	$\pm(y^2 - 104z^2)$ $\pm(8y^2 - 13z^2)$	124 125	$\pm(y^2 - 124z^2)$ $y^2 - 125z^2$
105	$\pm(y^2 - 105z^2)$ $\pm(3y^2 - 35z^2)$	126	$\pm(y^2 - 126z^2)$ $\pm(2y^2 - 63z^2)$
106	$y^2 - 106z^2$ $2y^2 - 53z^2$	127 128 129	$\pm(y^2 - 127z^2)$ $\pm(y^2 - 128z^2)$ $\pm(y^2 - 129z^2)$
107 108 109	$\pm(y^2 - 107z^2)$ $\pm(y^2 - 108z^2)$ $y^2 - 109z^2$	130	$y^2 - 130z^2$ $2y^2 - 65z^2$ $5y^2 - 26z^2$ $10y^2 - 13z^2$
110	$\pm(y^2 - 110z^2)$ $\pm(2y^2 - 55z^2)$		
111	$\pm(y^2 - 111z^2)$ $\pm(2y^2 + 2yz - 55z^2)$	131 132 133 134	$\pm(y^2 - 131z^2)$ $\pm(y^2 - 132z^2)$ $\pm(y^2 - 133z^2)$ $\pm(y^2 - 134z^2)$
112	$\pm(y^2 - 112z^2)$ $\pm(3y^2 + 2yz - 37z^2)$		
113	$y^2 - 113z^2$	135	$\pm(y^2 - 135z^2)$ $\pm(5y^2 - 27z^2)$
114	$\pm(y^2 - 114z^2)$ $\pm(3y^2 - 38z^2)$		
115	$\pm(y^2 - 115z^2)$ $\pm(5y^2 - 23z^2)$	136	$\pm(y^2 - 136z^2)$ $\pm(8y^2 - 17z^2)$ $\pm(3y^2 + 2yz - 45z^2)$

Tafel II.

Die einfachsten Ausdrücke der Formeln $Ly^2 + Myz + Nz^2$, in denen M ungerade ist, für alle Werte von $B = M^2 - 4LN$ von $B = 5$ bis $B = 305$.

Zahl B.	Reducierte Formel.
5	$y^2 + yz - z^2$
13	$y^2 + yz - 3z^2$
17	$y^2 + yz - 4z^2$
21	$\pm(y^2 + yz - 5z^2)$
29	$y^2 + yz - 7z^2$
33	$\pm(y^2 + yz - 8z^2)$
37	$y^2 + yz - 9z^2$
41	$y^2 + yz - 10z^2$
45	$\pm(y^2 + yz - 11z^2)$
53	$y^2 + yz - 13z^2$
57	$\pm(y^2 + yz - 14z^2)$
61	$y^2 + yz - 15z^2$
65	$y^2 + yz - 16z^2$ $2y^2 + yz - 8z^2$
69	$\pm(y^2 + yz - 17z^2)$
73	$y^2 + yz - 18z^2$
77	$y^2 + yz - 19z^2$
85	$y^2 + yz - 21z^2$ $3y^2 + yz - 7z^2$
89	$y^2 + yz - 22z^2$
93	$\pm(y^2 + yz - 23z^2)$
97	$y^2 + yz - 24z^2$
101	$y^2 + yz - 25z^2$
105	$\pm(y^2 + yz - 26z^2)$ $\pm(2y^2 + yz - 13z^2)$
109	$y^2 + yz - 27z^2$
113	$y^2 + yz - 28z^2$
117	$\pm(y^2 + yz - 29z^2)$
125	$y^2 + yz - 31z^2$
129	$\pm(y^2 + yz - 32z^2)$
133	$\pm(y^2 + yz - 33z^2)$
137	$y^2 + yz - 34z^2$
141	$\pm(y^2 + yz - 35z^2)$
145	$y^2 + yz - 36z^2$ $2y^2 + yz - 18z^2$ $4y^2 + yz - 9z^2$
149	$y^2 + yz - 37z^2$
153	$\pm(y^2 + yz - 38z^2)$
157	$\pm(y^2 + yz - 39z^2)$
161	$\pm(y^2 + yz - 40z^2)$
165	$\pm(y^2 + yz - 41z^2)$ $\pm(3y^2 + 3yz - 13z^2)$
173	$y^2 + yz - 43z^2$
177	$\pm(y^2 + yz - 44z^2)$
181	$y^2 + yz - 45z^2$
185	$y^2 + yz - 46z^2$ $2y^2 + yz - 23z^2$
189	$\pm(y^2 + yz - 47z^2)$
193	$y^2 + yz - 48z^2$
197	$y^2 + yz - 49z^2$
201	$\pm(y^2 + yz - 50z^2)$
205	$\pm(y^2 + yz - 51z^2)$ $\pm(3y^2 + yz - 17z^2)$
209	$\pm(y^2 + yz - 52z^2)$
213	$\pm(y^2 + yz - 53z^2)$
217	$\pm(y^2 + yz - 54z^2)$
221	$\pm(y^2 + yz - 55z^2)$ $\pm(5y^2 + yz - 11z^2)$
229	$y^2 + yz - 57z^2$ $3y^2 + yz - 19z^2$
233	$y^2 + yz - 58z^2$
237	$\pm(y^2 + yz - 59z^2)$
241	$y^2 + yz - 60z^2$
245	$\pm(y^2 + yz - 61z^2)$
249	$\pm(y^2 + yz - 62z^2)$
253	$\pm(y^2 + yz - 63z^2)$
257	$y^2 + yz - 64z^2$ $2y^2 + yz - 32z^2$
261	$\pm(y^2 + yz - 65z^2)$
265	$y^2 + yz - 66z^2$ $2y^2 + yz - 33z^2$
269	$y^2 + yz - 67z^2$
273	$\pm(y^2 + yz - 68z^2)$ $\pm(2y^2 + yz - 34z^2)$
277	$y^2 + yz - 69z^2$
281	$y^2 + yz - 70z^2$
285	$\pm(y^2 + yz - 71z^2)$ $\pm(3y^2 + 3yz - 23z^2)$
293	$y^2 + yz - 73z^2$
297	$\pm(y^2 + yz - 74z^2)$
301	$\pm(y^2 + yz - 75z^2)$
305	$\pm(y^2 + yz - 76z^2)$ $\pm(2y^2 + yz - 38z^2)$

Tafel III.

Teiler der Formel $t^2 - au^2$.

Formel.	Quadratische Teiler.	Lineare ungerade Teiler.
$t^2 - 2u^2$	$y^2 - 2z^2$	$8x + 1, 7.$
$t^2 - 3u^2$	$y^2 - 3z^2$ $3z^2 - y^2$	$12x + 1$ $12x + 11.$
$t^2 - 5u^2$	$y^2 - 5z^2$	$20x + 1, 9, 11, 19.$
$t^2 - 6u^2$	$y^2 - 6z^2$ $6z^2 - y^2$	$24x + 1, 19$ $24x + 5, 23.$
$t^2 - 7u^2$	$y^2 - 7z^2$ $7z^2 - y^2$	$28x + 1, 9, 25$ $28x + 3, 19, 27.$
$t^2 - 10u^2$	$y^2 - 10z^2$ $2y^2 - 5z^2$	$40x + 1, 9, 31, 39$ $40x + 3, 13, 27, 37.$
$t^2 - 11u^2$	$y^2 - 11z^2$ $11z^2 - y^2$	$44x + 1, 5, 9, 25, 37$ $44x + 7, 19, 35, 39, 43.$
$t^2 - 13u^2$	$y^2 - 13z^2$	$52x + 1, 3, 9, 17, 23; 25, 27, 29, 35, 43; 49, 51.$
$t^2 - 14u^2$	$y^2 - 14z^2$ $14z^2 - y^2$	$56x + 1, 9, 11, 25, 43, 51$ $56x + 5, 13, 31, 45, 47, 55.$
$t^2 - 15u^2$	$y^2 - 15z^2$ $15z^2 - y^2$ $3y^2 - 5z^2$ $5z^2 - 3y^2$	$60x + 1, 49$ $60x + 11, 59$ $60x + 7, 43$ $60x + 17, 53.$
$t^2 - 17u^2$	$y^2 - 17z^2$	$68x + 1, 9, 13, 15, 19; 21, 25, 33, 35, 43; 47, 49, 53, 55, 59; 67.$
$t^2 - 19u^2$	$y^2 - 19z^2$ $19z^2 - y^2$	$76x + 1, 5, 9, 17, 25; 45, 49, 61, 73$ $76x + 3, 15, 27, 31, 51; 59, 67, 71, 75.$
$t^2 - 21u^2$	$y^2 - 21z^2$ $21z^2 - y^2$	$84x + 1, 25, 37, 43, 67; 79$ $84x + 5, 17, 41, 47, 59; 83.$
$t^2 - 22u^2$	$y^2 - 22z^2$ $22z^2 - y^2$	$88x + 1, 3, 9, 25, 27; 49, 59, 67, 75, 81$ $88x + 7, 13, 21, 29, 39; 61, 63, 79, 85, 87.$

Formel.	Quadratische Teiler.	Lineare ungerade Teiler.
$t^2 - 23u^2$	$y^2 - 23z^2$	$92x + 1$, 9, 13, 25, 29; 41, 49, 73, 77, 81; 85
	$23z^2 - y^2$	$92x + 7$, 11, 15, 19, 43; 51, 63, 67, 79, 83; 91.
$t^2 - 26u^2$	$y^2 - 26z^2$	$104x + 1$, 9, 17, 23, 25; 49, 55, 79, 81, 87; 95, 103
	$2y^2 - 13z^2$	$104x + 5$, 11, 19, 21, 37; 45, 59, 67, 83, 85; 93, 99.
$t^2 - 29u^2$	$y^2 - 29z^2$	$116x + 1$, 5, 7, 9, 13; 23, 25, 33, 35, 45; 49, 51, 53, 57, 59; 63, 65, 67, 71, 81; 83, 91, 93, 103, 107; 109, 111, 115.
$t^2 - 30u^2$	$y^2 - 30z^2$	$120x + 1$, 19, 49, 91
	$30z^2 - y^2$	$120x + 29$, 71, 101, 119
	$2y^2 - 15z^2$	$120x + 17$, 83, 107, 113
	$15z^2 - 2y^2$	$120x + 7$, 13, 37, 103.
$t^2 - 31u^2$	$y^2 - 31z^2$	$124x + 1$, 5, 9, 25, 33; 41, 45, 49, 69, 81; 97, 101, 109, 113, 121.
	$31z^2 - y^2$	$124x + 3$, 11, 15, 23, 27; 43, 55, 75, 79, 83; 91, 99, 115, 119, 123.
$t^2 - 33u^2$	$y^2 - 33z^2$	$132x + 1$, 25, 31, 37, 49; 67, 91, 97, 103, 115
	$33z^2 - y^2$	$132x + 17$, 29, 35, 41, 65; 83, 95, 101, 107; 131.
$t^2 - 34u^2$	$y^2 - 34z^2$ $34z^2 - y^2$	$136x + 1$, 9, 15, 25, 33; 47, 49, 55, 81, 87; 89, 103, 111, 121, 127; 135
	$3y^2 + 2yz - 11z^2$ $11z^2 - 2yz - 3y^2$	$136x + 3$, 5, 11, 27, 29; 37, 45, 61, 75, 91; 99, 107, 109, 125, 131; 133.
$t^2 - 35u^2$	$y^2 - 35z^2$	$140x + 1$, 9, 29, 81, 109; 121
	$35z^2 - y^2$	$140x + 19$, 31, 59, 111, 131; 139
	$5y^2 - 7z^2$	$140x + 13$, 17, 33, 73, 97; 117
	$7z^2 - 5y^2$	$140x + 23$, 43, 67, 107, 123; 127.

Formel.	Quadratische Teiler.	Lineare ungerade Teiler.
$t^2 - 37u^2$	$y^2 - 37z^2$ $3y^2 + 2yz - 12z^2$	$148x + 1, 3, 7, 9, 11;\ 21, 25, 27, 33, 41;\ 47, 49, 53, 63, 65;\ 67, 71, 73, 75, 77;\ 81, 83, 85, 95, 99;\ 101, 107, 115, 121, 123;\ 127, 137, 139, 141, 145;\ 147.$
$t^2 - 38u^2$	$y^2 - 38z^2$	$152x + 1, 9, 11, 17, 25;\ 35, 43, 49, 73, 81;\ 83, 99, 115, 121, 123;\ 129, 137, 139$
	$38z^2 - y^2$	$152x + 13, 15, 23, 29, 31;\ 37, 53, 69, 71, 79;\ 103, 109, 117, 127, 135;\ 141, 143, 151.$
$t^2 - 39u^2$	$y^2 - 39z^2$	$156x + 1, 25, 49, 61, 121;\ 133$
	$39z^2 - y^2$	$156x + 23, 35, 95, 107, 131;\ 155$
	$2y^2 + 2yz - 19z^2$	$156x + 5, 41, 89, 125, 137;\ 149$
	$19z^2 - 2yz - 2y^2$	$156x + 7, 19, 31, 67, 115;\ 151.$
$t^2 - 41u^2$	$y^2 - 41z^2$	$164x + 1, 5, 9, 21, 23;\ 25, 31, 33, 37, 39;\ 43, 45, 49, 51, 57;\ 59, 61, 73, 77, 81;\ 83, 87, 91, 103, 105;\ 107, 113, 115, 119, 121;\ 125, 127, 131, 133, 139;\ 141, 143, 155, 159, 163.$
$t^2 - 42u^2$	$y^2 - 42z^2$	$168x + 1, 25, 79, 121, 127;\ 151$
	$42z^2 - y^2$	$168x + 17, 41, 47, 89, 143;\ 167$
	$2y^2 - 21z^2$	$168x + 11, 29, 53, 107, 149;\ 155$
	$21z^2 - 2y^2$	$168x + 13, 19, 61, 115, 139;\ 157.$
$t^2 - 43u^2$	$y^2 - 43z^2$	$172x + 1, 9, 13, 17, 21;\ 41, 49, 53, 57;\ 81, 97, 101, 109, 117;\ 121, 133, 145, 153, 165;\ 169$
	$43z^2 - y^2$	$172x + 3, 7, 19, 27, 39;\ 51, 55, 63, 71, 75;\ 91, 115, 119, 123, 131;\ 147, 151, 155, 159, 163;\ 171.$

Formel.	Quadratische Teiler.	Lineare ungerade Teiler.
$t^2 - 46u^2$	$y^2 - 46z^2$	$184x + 1, 3, 9, 25, 27; 35, 41, 49, 59, 73; 75, 81, 105, 121, 123; 131, 139, 147, 163, 169; 177, 179$
	$46z^2 - y^2$	$184x + 5, 7, 15, 21, 37; 45, 53, 61, 63, 79; 103, 109, 111, 125, 135; 143, 149, 157, 159, 175; 181, 183.$
$t^2 - 47u^2$	$y^2 - 47z^2$	$188x + 1, 9, 17, 21, 25; 37, 49, 53, 61, 65; 81, 89, 97, 101, 121; 145, 149, 153, 157, 165; 169, 173, 177$
	$47z^2 - y^2$	$188x + 11, 15, 19, 23, 31; 35, 39, 43, 67, 87; 91, 99, 107, 123, 127; 135, 139, 151, 163, 167; 171, 179, 187.$
$t^2 - 51u^2$	$y^2 - 51z^2$	$204x + 1, 13, 25, 49, 121; 145, 157, 169$
	$51z^2 - y^2$	$204x + 35, 47, 59, 83, 155; 179, 191, 203$
	$3y^2 - 17z^2$	$204x + 7, 31, 79, 91, 139; 163, 175, 199$
	$17z^2 - 3y^2$	$204x + 5, 29, 41, 65, 113; 125, 173, 197.$
$t^2 - 53u^2$	$y^2 - 53z^2$	$212x + 1, 7, 9, 11, 13; 15, 17, 25, 29, 37; 43, 47, 49, 57, 59; 63, 69, 77, 81, 89; 91, 93, 95, 97, 99; 105, 107, 113, 115, 117; 119, 121, 123, 131, 135; 143, 149, 153, 155, 163; 165, 169, 175, 183, 187; 195, 197, 199, 201, 203; 205, 211.$
$t^2 - 55u^2$	$y^2 - 55z^2$	$220x + 1, 9, 49, 69, 81; 89, 141, 169, 181, 201$
	$55z^2 - y^2$	$220x + 19, 39, 51, 79, 131; 139, 151, 171, 211, 219$
	$2y^2 + 2yz - 27z^2$	$220x + 13, 17, 57, 73, 117; 153, 173, 193, 197, 217$
	$27z^2 - 2yz - 2y^2$	$220x + 3, 23, 27, 47, 67; 103, 147, 163, 203, 207.$

Formel.	Quadratische Teiler.	Lineare ungerade Teiler.
$t^2 - 57u^2$	$y^2 - 57z^2$	$228x + 1$, 7, 25, 43, 49; 55, 61, 73, 85, 115; 121, 139, 157, 163, 169; 175, 187, 199
	$57z^2 - y^2$	$228x + 29$, 41, 53, 59, 65; 71, 89, 107, 113, 143; 155, 167, 173, 179, 185; 203, 221, 227.
$t^2 - 58u^2$	$y^2 - 58z^2$	$232x + 1$, 7, 9, 23, 25; 33, 49, 57, 63, 65; 71, 81, 103, 111, 121; 129, 151, 161, 167, 169; 175, 183, 199, 207, 209; 223, 225, 231
	$2y^2 - 29z^2$	$232x + 3$, 11, 19, 21, 27; 37, 43, 61, 69, 75; 77, 85, 99, 101, 131; 133, 147, 155, 157, 163; 171, 189, 195, 205, 211; 213, 221, 229.
$t^2 - 59u^2$	$y^2 - 59z^2$	$236x + 1$, 5, 9, 17, 21; 25, 29, 41, 45, 49; 53, 57, 81, 85, 105; 121, 125, 133, 137, 145; 153, 169, 181, 189, 193; 197, 205, 213, 225
	$59z^2 - y^2$	$236x + 11$, 23, 31, 39, 43; 47, 55, 67, 83, 91; 99, 103, 111, 115, 131; 151, 155, 179, 183, 187; 191, 195, 207, 211, 215; 219, 227, 231, 235.
$t^2 - 61u^2$	$y^2 - 61z^2$	$244x + 1$, 5, 7, 9, 11; 13, 23, 25, 31, 35; 41, 43, 45, 49, 51; 55, 57, 59, 63, 65; 67, 71, 73, 77, 79; 81, 87, 91, 97, 99; 109, 111, 113, 115, 117; 121, 125, 137, 139, 141; 143, 149, 151, 155, 159; 161, 169, 175, 191, 197; 205, 207, 211, 215, 217; 223, 225, 227, 229, 241.

Formel.	Quadratische Teiler.	Lineare ungerade Teiler.
$t^2 - 62u^2$	$y^2 - 62z^2$	$248x +$ 1, 9, 19, 25, 33; 35, 41, 49, 51, 59; 67, 81, 97, 103, 113; 121, 129, 131, 163, 169; 171, 187, 193, 195, 211; 219, 225, 227, 233, 235
	$62z^2 - y^2$	$248x +$ 13, 15, 21, 23, 29; 37, 53, 55, 61, 77; 79, 85, 117, 119, 127; 135, 141, 151, 167, 181; 189, 197, 199, 207, 213; 215, 223, 229, 239, 247.
$t^2 - 65u^2$	$y^2 - 65z^2$	$260x +$ 1, 9, 29, 49, 51; 61, 69, 79, 81, 101; 121, 129, 131, 139, 159; 179, 181, 191, 199, 209; 211, 231, 251, 259
	$5y^2 - 13z^2$	$260x +$ 7, 33, 37, 47, 57; 63, 67, 73, 83, 93; 97, 123, 137, 163, 167; 177, 187, 193, 197, 203; 213, 223, 227, 253.
$t^2 - 66u^2$	$y^2 - 66z^2$	$264x +$ 1, 25, 31, 49, 97; 103, 169, 199, 223, 247
	$66z^2 - y^2$	$264x +$ 17, 41, 65, 95, 161; 167, 215, 233, 239, 263
	$3y^2 - 22z^2$	$264x +$ 5, 53, 59, 125, 155; 179, 203, 221, 245, 251
	$22z^2 - 3y^2$	$264x +$ 13, 19, 43, 61, 85; 109, 139, 205, 211, 259.
$t^2 - 67u^2$	$y^2 - 67z^2$	$268x +$ 1, 9, 17, 21, 25; 29, 33, 37, 49, 65; 73, 77, 81, 89, 93; 121, 129, 149, 153, 157; 169, 173, 181, 189, 193; 205, 217, 225, 237, 241; 257, 261, 265.
	$67z^2 - y^2$	$268x +$ 3, 7, 11, 27, 31; 43, 51, 63, 75, 79; 87, 95, 99, 111, 115; 119, 139, 147, 175, 179; 187, 191, 195, 203, 219; 231, 235, 239, 243, 247; 251, 259, 267.

Formel.	Quadratische Teiler.	Lineare ungerade Teiler.
$t^2 - 69u^2$	$y^2 - 69z^2$	$276x + 1$, 13, 25, 31, 49; 55, 73, 85, 121, 127; 133, 139, 151, 163, 169; 187, 193, 211, 223, 259; 265, 271
	$69z^2 - y^2$	$276x + 5$, 11, 17, 53, 65; 83, 89, 107, 113, 125; 137, 143, 149, 155, 191; 203, 221, 227, 245, 251; 263, 275.
$t^2 - 70u^2$	$y^2 - 70z^2$	$280x + 1$, 9, 11, 51, 81; 99, 121, 169, 179, 211; 219, 249
	$70z^2 - y^2$	$280x + 31$, 61, 69, 101, 111; 159, 181, 199, 229, 269; 271, 279
	$2y^2 - 35z^2$	$280x + 23$, 37, 53, 93, 127; 183, 197, 207, 247, 253; 263, 277
	$35z^2 - 2y^2$	$280x + 3$, 17, 27, 33, 73; 83, 97, 153, 187, 227; 243, 257.
$t^2 - 71u^2$	$y^2 - 71z^2$	$284x + 1$, 5, 9, 25, 29; 37, 45, 49, 57, 73; 77, 81, 89, 101, 109; 121, 125, 129, 145, 157; 161, 169, 185, 217, 221; 225, 229, 233, 237, 245; 249, 253, 261, 273, 277
	$71z^2 - y^2$	$284x + 7$, 11, 23, 31, 35; 39, 47, 51, 55, 59; 63, 67, 99, 115, 123; 127, 139, 155, 159, 163; 175, 183, 195, 203, 207; 211, 227, 235, 239, 247; 255, 259, 275, 279, 283.
$t^2 - 73u^2$	$y^2 - 73z^2$	$292x + 1$, 3, 9, 19, 23; 25, 27, 35, 37, 41; 49, 55, 57, 61, 65; 67, 69, 71, 75, 77; 79, 81, 85, 89, 91; 97, 105, 109, 111, 119; 121, 123, 127, 137, 143; 145, 147, 149, 155, 165; 169, 171, 173, 181, 183; 187, 195, 201, 203, 207; 211, 213, 215, 217, 221; 223, 225, 227, 231, 235; 237, 243, 251, 255, 257; 265, 267, 269, 273, 283; 289, 291.

Formel.	Quadratische Teiler.	Lineare ungerade Teiler.
$t^2 - 74u^2$	$y^2 - 74z^2$	$296x + 1$, 7, 9, 25, 33; 41, 47, 49, 63, 65; 71, 73, 81, 95, 121; 127, 137, 145, 151, 159; 169, 175, 201, 215, 223; 225, 231, 233, 247, 249; 255, 263, 271, 287, 289; 295
	$2y^2 - 37z^2$	$296x + 5$, 13, 19, 29, 35; 43, 45, 51, 59, 61; 69, 91, 93, 109, 117; 125, 131, 133, 163, 165; 171, 179, 187, 203, 205; 227, 235, 237, 245, 251; 253, 261, 267, 277, 283; 291.
$t^2 - 77u^2$	$y^2 - 77z^2$	$308x + 1$, 9, 15, 23, 25; 37, 53, 67, 71, 81; 93, 113, 135, 141, 155; 163, 169, 177, 179, 191; 207, 221, 225, 235, 247; 255, 267, 289, 291, 295
	$77z^2 - y^2$	$308x + 13$, 17, 19, 41, 53; 61, 73, 83, 87, 101; 117, 129, 131, 139, 145; 153, 167, 173, 195, 215; 227, 237, 241, 255, 271; 283, 285, 293, 299, 307.
$t^2 - 78u^2$	$y^2 - 78z^2$	$312x + 1$, 25, 43, 49, 121; 139, 211, 217, 235, 259; 283, 289
	$78z^2 - y^2$	$312x + 23$, 29, 53, 77, 95; 101, 173, 191, 263, 269; 287, 311
	$2y^2 - 39z^2$	$312x + 11$, 41, 59, 83, 89; 137, 161, 203, 227, 275; 281, 305
	$39z^2 - 2y^2$	$312x + 7$, 31, 37, 85, 109; 151, 175, 223, 229, 253; 271, 301.
$t^2 - 79u^2$	$y^2 - 79z^2$ $26y^2 + 2yz - 3z^2$	$316x + 1$, 5, 9, 13, 21; 25, 45, 49, 65, 73; 81, 89, 97, 101, 105; 117, 121, 125, 129, 141; 169, 177, 181, 189, 209; 213, 225, 241, 245, 253; 257, 269, 273, 277, 281; 289, 301, 309, 313
	$79z^2 - y^2$ $3z^2 - 2yz - 26y^2$	$316x + 3$, 7, 15, 27, 35; 39, 43, 47, 59, 63; 71, 75, 91, 103, 107; 127, 135, 139, 147, 175; 187, 191, 195, 199, 211; 215, 219, 227, 235, 243; 251, 267, 271, 291, 295; 303, 307, 311, 315.

Tafel IV.

Teiler der Formel $t^2 + au^2$, wo a eine Zahl von der Form $4n + 1$ ist.

Formel.	Quadratische Teiler.	Lineare ungerade Teiler.
$t^2 + u^2$	$y^2 + z^2$	$4x + 1$.
$t^2 + 5u^2$	$y^2 + 2yz + 6z^2$ $2y^2 + 2yz + 3z^2$	$20x + 1, 9$ $20x + 3, 7$
$t^2 + 13u^2$	$y^2 + 2yz + 14z^2$ $2y^2 + 2yz + 7z^2$	$52x + 1, 9, 17, 25, 29; 49$ $52x + 7, 11, 15, 19, 31; 47$
$t^2 + 17u^2$	$y^2 + 2yz + 18z^2$ $2y^2 + 2yz + 9z^2$ $3y^2 + 2yz + 6z^2$	$68x + 1, 9, 13, 21, 25; 33, 49, 53$ $68x + 3, 7, 11, 23, 27; 31, 39, 63$
$t^2 + 21u^2$	$y^2 + 2yz + 22z^2$ $2y^2 + 2yz + 11z^2$ $5y^2 + 6yz + 6z^2$ $10y^2 + 6yz + 3z^2$	$84x + 1, 25, 37$ $84x + 11, 23, 71$ $84x + 5, 17, 41$ $84x + 19, 31, 55$.
$t^2 + 29u^2$	$y^2 + 2yz + 30z^2$ $5y^2 + 2yz + 6z^2$ $2y^2 + 2yz + 15z^2$ $10y^2 + 2yz + 3z^2$	$116x + 1, 5, 9, 13, 25; 33, 45, 49, 53, 57; 65, 81, 93, 109$ $116x + 3, 11, 15, 19, 27; 31, 39, 43, 47, 55; 75, 79, 95, 99$.
$t^2 + 33u^2$	$y^2 + 2yz + 34z^2$ $2y^2 + 2yz + 17z^2$ $3y^2 + 6yz + 14z^2$ $6y^2 + 6yz + 7z^2$	$132x + 1, 25, 37, 49, 97$ $132x + 17, 29, 41, 65, 101$ $132x + 23, 47, 59, 71, 119$ $132x + 7, 19, 43, 79, 127$.
$t^2 + 37u^2$	$y^2 + 2yz + 38z^2$ $2y^2 + 2yz + 19z^2$	$148x + 1, 9, 21, 25, 33; 41, 49, 53, 65, 73; 77, 81, 85, 101, 121; 137, 141, 145$ $148x + 15, 19, 23, 31, 35; 39, 43, 51, 55, 59; 79, 87, 91, 103, 119; 131, 135, 143$.
$t^2 + 41u^2$	$y^2 + 2yz + 42z^2$ $2y^2 + 2yz + 21z^2$ $5y^2 + 6yz + 10z^2$ $3y^2 + 2yz + 14z^2$ $6y^2 + 2yz + 7z^2$	$164x + 1, 5, 9, 21, 25; 33, 37, 45, 49, 57; 61, 73, 77, 81, 105; 113, 121, 125, 133, 141$ $164x + 3, 7, 11, 15, 19; 27, 35, 47, 55, 63; 67, 71, 75, 79, 95; 99, 111, 135, 147, 151$.

Formel.	Quadratische Teiler.	Ungerade lineare Teiler.
$t^2 + 53u^2$	$y^2 + 2yz + 54z^2$ $9y^2 + 2yz + 6z^2$	$212x$ + 1, 9, 13, 17, 25; 29, 37, 49, 57, 69; 77, 81, 89, 93, 97; 105, 113, 117, 121, 149; 153, 165, 169, 197, 201; 205
	$2y^2 + 2yz + 27z^2$ $18y^2 + 2yz + 3z^2$	$212x$ + 3, 19, 23, 27, 31; 35, 39, 51, 55, 67; 71, 75, 79, 83, 87; 103, 111, 127, 139, 147; 151, 167, 171, 179, 191; 207.
$t^2 + 57u^2$	$y^2 + 2yz + 58z^2$	$228x$ + 1, 25, 49, 61, 73; 85, 121, 157, 169
	$2y^2 + 2yz + 29z^2$	$228x$ + 29, 41, 53, 65, 89; 113, 173, 185, 221
	$3y^2 + 6yz + 22z^2$	$228x$ + 31, 67, 79, 91, 103; 127, 151, 211, 223
	$6y^2 + 6yz + 11z^2$	$228x$ + 11, 23, 35, 47, 83; 119, 131, 191, 215.
$t^2 + 61u^2$	$y^2 + 2yz + 62z^2$ $5y^2 + 6yz + 14z^2$	$244x$ + 1, 5, 9, 13, 25; 41, 45, 49, 57, 65; 73, 77, 81, 97, 109; 113, 117, 121, 125, 137; 141, 149, 161, 169, 197; 205, 217, 225, 229, 241
	$2y^2 + 2yz + 31z^2$ $10y^2 + 6yz + 7z^2$	$244x$ + 7, 11, 23, 31, 35; 43, 51, 55, 59, 63; 67, 71, 79, 87, 91; 99, 111, 115, 139, 143; 151, 155, 159, 175, 191; 207, 211, 215, 223, 227.
$t^2 + 65u^2$	$y^2 + 2yz + 66z^2$ $9y^2 + 10yz + 10z^2$	$260x$ + 1, 9, 29, 49, 61; 69, 81, 101, 121, 129; 181, 209
	$2y^2 + 2yz + 33z^2$ $18y^2 + 10yz + 5z^2$	$260x$ + 33, 37, 57, 73, 93; 97, 137, 177, 193, 197; 213, 253.
	$3y^2 + 2yz + 22z^2$	$260x$ + 3, 23, 27, 43, 87; 103, 107, 127, 147, 183; 207, 243
	$6y^2 + 2yz + 11z^2$	$260x$ + 11, 19, 31, 59, 71; 99, 111, 119, 151, 171; 219, 239.

Formel.	Quadratische Teiler.	Ungerade lineare Teiler.
$t^2 + 69u^2$	$y^2 + 2yz + 70z^2$ $13y^2 + 6yz + 6z^2$	$276x +$ 1, 13, 25, 49, 73; 85, 121, 133, 169, 193; 265
	$5y^2 + 2yz + 14z^2$	$276x +$ 5, 17, 53, 65, 89; 113, 125, 137, 149, 221; 245.
	$2y^2 + 2yz + 35z^2$ $26y^2 + 6yz + 3z^2$	$276x +$ 35, 47, 59, 71, 95; 119, 131, 167, 179, 215; 239
	$10y^2 + 2yz + 7z^2$	$276x +$ 7, 19, 43, 67, 79; 91, 103, 175, 199, 235; 247.
$t^2 + 73u^2$	$y^2 + 2yz + 74z^2$ $2y^2 + 2yz + 37z^2$	$292x +$ 1, 9, 25, 37, 41; 49, 57, 61, 65, 69; 77, 81, 85, 89, 97; 105, 109, 121, 137, 145; 149, 165, 169, 173, 181; 201, 213, 217, 221, 225; 237, 257, 265, 269, 273; 289.
	$7y^2 + 10yz + 14z^2$	$292x +$ 7, 11, 15, 31, 39; 43, 47, 51, 59, 63; 83, 87, 95, 99, 103; 107, 115, 131, 135, 139; 151, 159, 163, 167, 175; 179, 191, 199, 239, 247; 259, 263, 271, 275, 279; 287.
$t^2 + 77u^2$	$y^2 + 2yz + 78z^2$ $9y^2 + 14yz + 14z^2$	$308x +$ 1, 9, 25, 37, 53; 81, 93, 113, 137, 141; 169, 177, 221, 225, 289
	$13y^2 + 2yz + 6z^2$	$308x +$ 13, 17, 41, 73, 89; 101, 117, 129, 145, 149; 173, 241, 257, 285, 293.
	$2y^2 + 2yz + 39z^2$ $18y^2 + 14yz + 7z^2$	$308x +$ 39, 43, 51, 79, 95; 107, 123, 127, 151, 183; 211, 219, 239, 263, 303
	$26y^2 + 2yz + 3z^2$	$308x +$ 3, 27, 31, 47, 59; 75, 103, 111, 115, 159; 199, 223, 243, 251, 279.

Formel.	Quadratische Teiler.	Ungerade lineare Teiler.
$t^2 + 85u^2$	$y^2 + 2yz + 86z^2$	$340x +$ 1, 9, 21, 49, 69; 81, 89, 101, 121, 149; 161, 169, 189, 229, 281; 321
	$5y^2 + 10yz + 22z^2$	$340x +$ 37, 57, 73, 97, 113; 133, 173, 177, 193, 197; 233, 277, 313, 317, 333; 337
	$2y^2 + 2yz + 43z^2$	$340x +$ 43, 47, 67, 83, 87; 103, 123, 127, 183, 203; 223, 247, 263, 287, 307; 327
	$10y^2 + 10yz + 11z^2$	$340x +$ 11, 31, 39, 71, 79; 91, 99, 131, 139, 159; 199, 211, 231, 279, 299; 311
$t^2 + 89u^2$	$y^2 + 2yz + 90z^2$ $2y^2 + 2yz + 45z^2$ $5y^2 + 2yz + 18z^2$ $10y^2 + 2yz + 9z^2$	$356x +$ 1, 5, 9, 17, 21; 25, 45, 49, 53, 57; 69, 73, 81, 85, 93; 97, 105, 109, 121, 125; 129, 133, 153, 157, 161; 169, 173, 177, 189, 217; 225, 233, 245, 249, 257; 265, 269, 277, 285, 289; 301, 309, 317, 345
	$3y^2 + 2yz + 30z^2$ $6y^2 + 2yz + 15z^2$ $7y^2 + 6yz + 14z^2$	$356x +$ 3, 7, 15, 19, 23; 27, 31, 35, 43, 51; 59, 63, 75, 83, 95; 103, 115, 119, 127, 135; 143, 147, 151, 155, 159; 163, 171, 175, 191, 207; 211, 215, 219, 239, 243; 255, 279, 291, 295, 315; 319, 323, 327, 343.
$t^2 + 93u^2$	$y^2 + 2yz + 94z^2$	$372x +$ 1, 25, 49, 97, 109; 121, 133, 157, 169, 193; 205, 253, 289, 349, 361
	$17y^2 + 6yz + 6z^2$	$372x +$ 17, 29, 53, 65, 77; 89, 137, 161, 185, 197; 209, 269, 305, 353, 365
	$2y^2 + 2yz + 47z^2$	$372x +$ 35, 47, 59, 71, 95; 107, 131, 143, 191, 227; 287, 299, 311, 335, 359
	$34y^2 + 6yz + 3z^2$	$372x +$ 43, 55, 79, 91, 115; 127, 139, 151, 199, 223; 247, 259, 271, 331, 367

Formel.	Quadratische Teiler.	Ungerade lineare Teiler.
$t^2 + 97u^2$	$y^2 + 2yz + 98z^2$ $2y^2 + 2yz + 49z^2$	$388x +$ 1, 9, 25, 33, 49; 53, 61, 65, 73, 81; 85, 89, 93, 101, 105; 109, 113, 121, 129, 133; 141, 145, 161, 169, 185; 193, 197, 205, 221, 225; 229, 237, 241, 269, 273; 285, 289, 293, 297, 309; 313, 341, 345, 353, 357; 361, 377, 385
	$7y^2 + 2yz + 14z^2$	$388x +$ 7, 15, 19, 23, 39; 51, 55, 59, 63, 67; 71, 83, 87, 107, 111; 123, 127, 131, 135, 139; 143, 155, 171, 175, 179; 187, 199, 207, 211, 215; 223, 231, 235, 239, 251; 263, 271, 311, 319, 331; 343, 347, 351, 359, 367; 371, 375, 383.
$t^2 + 101u^2$	$y^2 + 2yz + 102z^2$ $5y^2 + 6yz + 22z^2$ $17y^2 + 2yz + 6z^2$ $9y^2 + 10yz + 14z^2$	$404x +$ 1, 5, 9, 13, 17; 21, 25, 33, 37, 45; 49, 65, 77, 81, 85; 97, 105, 117, 121, 125; 137, 153, 157, 165, 169; 177, 181, 185, 189, 193; 197, 201, 221, 225, 233; 245, 249, 273, 281, 289; 297, 305, 313, 321, 329; 357, 361, 373, 381, 385
	$2y^2 + 2yz + 51z^2$ $10y^2 + 6yz + 11z^2$ $34y^2 + 2yz + 3z^2$ $18y^2 + 10yz + 7z^2$	$404x +$ 3, 7, 11, 15, 27; 35, 39, 51, 55, 59; 63, 67, 75, 83, 91; 99, 103, 111, 119, 127; 135, 139, 143, 147, 151; 163, 167, 175, 187, 191; 195, 199, 231, 243, 255; 259, 263, 271, 275, 291; 295, 311, 315, 331, 335; 343, 347, 351, 363, 375
$t^2 + 105u^2$	$y^2 + 2yz + 106z^2$	$420x +$ 1, 109, 121, 169, 289, 361
	$2y^2 + 2yz + 53z^2$	$420x +$ 53, 113, 137, 197, 233, 317
	$10y^2 + 10yz + 13z^2$	$420x +$ 13, 73, 97, 157, 313, 397
	$5y^2 + 10yz + 26z^2$	$420x +$ 41, 89, 101, 209, 269, 341
	$3y^2 + 6yz + 38z^2$	$420x +$ 47, 83, 143, 167, 227, 383
	$6y^2 + 6yz + 19z^2$	$420x +$ 19, 31, 139, 199, 271, 391
	$7y^2 + 14yz + 22z^2$	$420x +$ 43, 67, 127, 163, 247, 403
	$14y^2 + 14yz + 11z^2$	$420x +$ 11, 71, 179, 191, 239, 359.

Tafel V.

Teiler der Formel $t^2 + au^2$, in welcher a eine Zahl von der Form $4n + 3$ ist.

Formel.	Quadratische Teiler.	Ungerade lineare Teiler.
$t^2 + 3u^2$	$y^2 + yz + z^2$	$6x + 1.$
$t^2 + 7u^2$	$y^2 + 7z^2$	$14x + 1, 9, 11.$
$t^2 + 11u^2$	$y^2 + yz + 3z^2$	$22x + 1, 3, 5, 9, 15.$
$t^2 + 15u^2$	$y^2 + 15z^2$ $3y^2 + 5z^2$	$30x + 1, 19$ $30x + 17, 23$
$t^2 + 19u^2$	$y^2 + yz + 5z^2$	$38x + 1, 5, 7, 9, 11; 17, 23, 25, 35.$
$t^2 + 23u^2$	$y^2 + 23z^2$ $3y^2 + 2yz + 8z^2$	$46x + 1, 3, 9, 13, 25; 27, 29, 31,$ $35, 39; 41.$
$t^2 + 31u^2$	$y^2 + 31z^2$ $5y^2 + 4yz + 7z^2$	$62x + 1, 5, 7, 9, 19; 25, 33, 35,$ $39, 41; 45, 47, 49, 51, 59.$
$t^2 + 35u^2$	$y^2 + yz + 9z^2$ $3y^2 + yz + 3z^2$	$70x + 1, 9, 11, 29, 39, 51$ $70x + 3, 13, 17, 27, 33, 47.$
$t^2 + 39u^2$	$y^2 + 39z^2$ $3y^2 + 13z^2$ $5y^2 + 2yz + 8z^2$	$78x + 1, 25, 43, 49, 55, 61$ $78x + 5, 11, 41, 47, 59, 71.$
$t^2 + 43u^2$	$y^2 + yz + 11z^2$	$86x + 1, 9, 11, 13, 15; 17, 21, 23,$ $25, 31; 35, 41, 47, 49, 53;$ $57, 59, 67, 79, 81; 83.$
$t^2 + 47u^2$	$y^2 + 47z^2$ $3y^2 + 2yz + 16z^2$ $7y^2 + 6yz + 8z^2$	$94x + 1, 3, 7, 9, 17; 21, 25, 27,$ $37, 49; 51, 53, 55, 59, 61;$ $63, 65, 71, 75, 79; 81, 83, 89.$
$t^2 + 51u^2$	$y^2 + yz + 13z^2$ $3y^2 + 3yz + 5z^2$	$102x + 1, 13, 19, 25, 43; 49, 55, 67$ $102x + 5, 11, 23, 29, 41; 65, 71, 95.$
$t^2 + 55u^2$	$y^2 + 55z^2$ $5y^2 + 11z^2$ $7y^2 + 2yz + 8z^2$	$110x + 1, 9, 31, 49, 59; 69, 71, 81,$ $89, 91$ $110x + 7, 13, 17, 43, 57; 63, 73,$ $83, 87, 107.$

Formel.	Quadratische Teiler.	Ungerade lineare Teiler.
t^2+59u^2	$y^2+yz+15z^2$ $3y^2+yz+5z^2$	$118x+1, 3, 5, 7, 9; 15, 17, 19, 21, 25; 27, 29, 35, 41, 45; 49, 51, 53, 57, 63; 71, 75, 79, 81, 85; 87, 95, 105, 107.$
t^2+67u^2	$y^2+yz+17z^2$	$134x+1, 9, 15, 17, 19; 21, 23, 25, 29, 33; 35, 37, 39, 47, 49; 55, 59, 65, 71, 73; 77, 81, 83, 89, 91; 93, 103, 107, 121, 123; 127, 129, 131.$
t^2+71u^2	y^2+71z^2 $3y^2+2yz+24z^2$ $9y^2+2yz+8z^2$ $5y^2+4yz+15z^2$	$142x+1, 3, 5, 9, 15; 19, 25, 27, 29, 37; 43, 45, 49, 57, 73; 75, 77, 79, 81, 83; 87, 89, 91, 95, 101; 103, 107, 109, 111, 119; 121, 125, 129, 131, 135.$
t^2+79u^2	y^2+79z^2 $5y^2+2yz+16z^2$ $11y^2+6yz+8z^2$	$158x+1, 5, 9, 11, 13; 19, 21, 23, 25, 31; 45, 49, 51, 55, 65; 67, 73, 81, 83, 87; 89, 95, 97, 99, 101; 105, 111, 115, 117, 119; 121, 123, 125, 129, 131; 141, 143, 151, 155.$
t^2+83u^2	$y^2+yz+21z^2$ $3y^2+yz+7z^2$	$166x+1, 3, 7, 9, 11; 17, 21, 23, 25, 27; 29, 31, 33, 37, 41; 49, 51, 59, 61, 63; 65, 69, 75, 77, 81; 87, 93, 95, 99, 109; 111, 113, 119, 121, 123; 127, 131, 147, 151, 153; 161.$
t^2+87u^2	y^2+87z^2 $7y^2+4yz+13z^2$ $3y^2+29z^2$ $11y^2+2yz+8z^2$	$174x+1, 7, 13, 25, 49; 67, 91, 103, 109, 115; 121, 139, 151, 169.$ $174x+11, 17, 41, 47, 77; 89, 95, 101, 113, 119; 131, 137, 143, 155.$
t^2+91u^2	$y^2+yz+23z^2$ $5y^2+3yz+5z^2$	$182x+1, 9, 23, 25, 29; 43, 51, 53, 79, 81; 95, 107, 113, 121, 127; 155, 165, 179.$ $182x+5, 7, 19, 31, 33; 41, 45, 47, 59, 73; 83, 89, 97, 111, 125; 145, 167, 171.$

Formel.	Quadratische Teiler.	Ungerade lineare Teiler.
$t^2 + 95u^2$	$y^2 + 95z^2$ $5y^2 + 19z^2$ $9y^2 + 4yz + 11z^2$ $3y^2 + 2yz + 32z^2$ $13y^2 + 6yz + 8z^2$	$190x +$ 1, 9, 11, 39, 49; 61, 81, 99, 101, 111; 119, 121, 131, 139, 149: 159, 161, 169 $190x +$ 3, 13, 27, 33, 37; 53, 67, 97, 103, 107; 113, 117, 127, 143, 147; 167, 173, 183.
$t^2 + 103u^2$	$y^2 + 103z^2$ $13y^2 + 2yz + 8z^2$ $7y^2 + 6yz + 16z^2$	$206x +$ 1, 7, 9, 13, 15; 17, 19, 23, 25, 29; 33, 41, 49, 55, 59; 61, 63, 79, 81, 83; 91, 93, 97, 105, 107; 111, 117, 119, 121, 129; 131, 133, 135, 137, 139; 141, 149, 153, 155, 159; 161, 163, 167, 169, 171; 175, 179, 185, 195, 201; 203.

Tafel VI.

Teiler der Formel $t^2 + 2au^2$, in welcher a eine Zahl von der Form $4n + 1$ ist.

Formel.	Quadratische Teiler.	Ungerade lineare Teiler.
$t^2 + 2u^2$	$y^2 + 2z^2$	$8x +$ 1, 3.
$t^2 + 10u^2$	$y^2 + 10z^2$ $2y^2 + 5z^2$	$40x +$ 1, 9, 11, 19 $40x +$ 7, 13, 23, 37
$t^2 + 26u^2$	$y^2 + 26z^2$ $3y^2 + 4yz + 10z^2$ $2y^2 + 13z^2$ $6y^2 + 4yz + 5z^2$	$104x +$ 1, 3, 9, 17, 25; 27, 35, 43, 49, 51; 75, 81 $104x +$ 5, 7, 15, 21, 31; 37, 45, 47, 63, 71; 85, 93.
$t^2 + 34u^2$	$y^2 + 34z^2$ $2y^2 + 17z^2$ $5y^2 + 8yz + 10z^2$	$136x +$ 1, 9, 19, 25, 33; 35, 43, 49, 59, 67; 81, 83, 89, 115, 121; 123 $136x +$ 5, 7, 23, 29, 31; 37, 39, 45, 61, 63; 71, 79, 95, 109, 125; 133.

Formel.	Quadratische Teiler.	Ungerade lineare Teiler.
$t^2 + 42u^2$	$y^2 + 42z^2$	$168x +$ 1, 25, 43, 67, 121, 163
	$3y^2 + 14z^2$	$168x +$ 17, 41, 59, 83, 89, 131
	$6y^2 + 7z^2$	$168x +$ 13, 31, 55, 61, 103, 157
	$2y^2 + 21z^2$	$168x +$ 23, 29, 53, 71, 95, 149.
$t^2 + 58u^2$	$y^2 + 58z^2$	$232x +$ 1, 9, 25, 33, 35; 49, 51, 57, 59, 65; 67, 81, 83, 91, 107; 115, 121, 123, 129, 139; 161, 169, 179, 187, 209; 219, 225, 227.
	$2y^2 + 29z^2$	$232x +$ 15, 21, 31, 37, 39; 47, 55, 61, 69, 77; 79, 85, 95, 101, 119; 127, 133, 135, 143, 157; 159, 189, 191, 205, 213; 215, 221, 229.
$t^2 + 66u^2$	$y^2 + 66z^2$ $3y^2 + 22z^2$	$264x +$ 1, 25, 49, 67, 91; 97, 115, 163, 169, 235
	$2y^2 + 33z^2$ $6y^2 + 11z^2$	$264x +$ 17, 35, 41, 65, 83; 107, 131, 161, 227, 233.
	$5y^2 + 4yz + 14z^2$	$264x +$ 5, 23, 47, 53, 71; 119, 125, 191, 221, 245
	$10y^2 + 4yz + 7z^2$	$264x +$ 7, 13, 61, 79, 85; 109, 127, 151, 175, 205.
$t^2 + 74u^2$	$y^2 + 74z^2$ $3y^2 + 4yz + 26z^2$ $9y^2 + 8yz + 10z^2$	$296x +$ 1, 9, 11, 25, 27; 33, 41, 49, 65, 67; 73, 75, 81, 83, 99; 107, 115, 121, 123, 137; 139, 145, 147, 155, 169; 195, 201, 211, 219, 225; 233, 243, 249, 275, 289; 299
	$2y^2 + 37z^2$ $6y^2 + 4yz + 13z^2$ $18y^2 + 8yz + 5z^2$	$296x +$ 5, 13, 15, 23, 29; 31, 39, 45, 55, 61; 69, 79, 87, 93, 103; 109, 117, 119, 125, 133; 135, 143, 165, 167, 183; 191, 199, 205, 207, 237; 239, 245, 253, 261, 277; 279.

Formel.	Quadratische Teiler.	Ungerade lineare Teiler.
$t^2 + 82u^2$	$y^2 + 82z^2$ $2y^2 + 41z^2$	$328x +$ 1, 9, 25, 33, 43; 49, 51, 57, 59, 73; 81, 83, 91, 105, 107; 113, 115, 121, 131, 139; 155, 163, 169, 185, 187; 195, 201, 203, 209, 225; 241, 251, 267, 283, 289; 291, 297, 305, 307, 323.
	$7y^2 + 8yz + 14z^2$	$328x +$ 7, 13, 15, 29, 47; 53, 55, 63, 69, 71; 79, 85, 93, 95, 101; 109, 111, 117, 135, 149; 151, 157, 167, 175, 181; 183, 191, 199, 229, 231; 239, 253, 261, 263, 293; 301, 309, 311, 317, 325.
$t^2 + 106u^2$	$y^2 + 106z^2$ $11y^2 + 4yz + 10z^2$	$424x +$ 1, 9, 11, 17, 25; 43, 49, 57, 59, 81; 89, 91, 97, 99, 105; 107, 113, 115, 121, 123; 131, 153, 155, 163, 169; 187, 195, 201, 203, 211; 219, 225, 227, 241, 249; 259, 275, 281, 289, 305; 307, 329, 331, 347, 355; 361, 377, 387, 395, 409; 411, 417.
	$2y^2 + 53z^2$ $22y^2 + 4yz + 5z^2$	$424x +$ 5, 21, 23, 31, 39; 45, 55, 61, 71, 79; 85, 87, 101, 103, 109; 111, 125, 127, 133, 141; 151, 157, 167, 173, 181; 189, 191, 207, 215, 231; 239, 245, 247, 253, 263; 277, 279, 285, 287, 295; 341, 349, 351, 357, 359; 373, 383, 389, 391, 397; 405, 421.

Tafel VII.

Teiler der Formel $t^2 + 2au^2$, in welcher a eine Zahl von der Form $4n + 3$ ist.

Formel.	Quadratische Teiler.	Ungerade lineare Teiler.
$t^2 + 6u^2$	$y^2 + 6z^2$	$24x + 1, 7$
	$2y^2 + 3z^2$	$24x + 5, 11.$
$t^2 + 14u^2$	$y^2 + 14z^2$ $2y^2 + 7z^2$	$56x + 1, 9, 15, 23, 25, 39$
	$3y^2 + 4yz + 6z^2$	$56x + 3, 5, 13, 19, 27, 45.$
$t^2 + 22u^2$	$y^2 + 22z^2$	$88x + 1, 9, 15, 23, 25; 31, 47, 49, 71, 81$
	$2y^2 + 11z^2$	$88x + 13, 19, 21, 29, 35; 43, 51, 61, 83, 85.$
$t^2 + 30u^2$	$y^2 + 30z^2$	$120x + 1, 31, 49, 79$
	$2y^2 + 15z^2$	$120x + 17, 23, 47, 113$
	$5y^2 + 6z^2$	$120x + 11, 29, 59, 101$
	$10y^2 + 3z^2$	$120x + 13, 37, 43, 67.$
$t^2 + 38u^2$	$y^2 + 38z^2$ $6y^2 + 4yz + 7z^2$	$152x + 1, 7, 9, 17, 23; 25, 39, 47, 49, 55; 63, 73, 81, 87, 111; 119, 121, 137$
	$2y^2 + 19z^2$ $3y^2 + 4yz + 14z^2$	$152x + 3, 13, 21, 27, 29; 37, 51, 53, 59, 67; 69, 75, 91, 107, 109; 117, 141, 147.$
$t^2 + 46u^2$	$y^2 + 46z^2$ $2y^2 + 23z^2$	$184x + 1, 9, 25, 31, 39; 41, 47, 49, 55, 71; 73, 81, 87, 95, 105; 119, 121, 127, 151, 167; 169, 177$
	$5y^2 + 4yz + 10z^2$	$184x + 5, 11, 19, 21, 37; 43, 45, 51, 53, 61; 67, 83, 91, 99, 107; 109, 125, 149, 155, 157; 171, 181.$

Formel.	Qnadratische Teiler.	Ungerade lineare Teiler.
$t^2 + 62u^2$	$y^2 + 62z^2$ $2y^2 + 31z^2$ $7y^2 + 12yz + 14z^2$	$248x +$ 1, 7, 9, 25, 33; 39, 41, 47, 49, 63; 71, 81, 87, 95, 97; 103, 111, 113, 121, 129; 143, 159, 169, 175, 183; 191, 193, 225, 231, 233
	$6y^2 + 4yz + 11z^2$ $3y^2 + 4yz + 22z^2$	$248x +$ 3, 11, 13, 21, 27; 29, 37, 43, 53, 61; 75, 77, 83, 85, 91; 99, 115, 117, 123, 139; 141, 147, 179, 181, 189; 197, 203, 213, 229, 243.
$t^2 + 70u^2$	$y^2 + 70z^2$	$280x +$ 1, 9, 39, 71, 79; 81, 121, 151, 169, 191; 239, 249
	$10y^2 + 7z^2$	$280x +$ 17, 33, 47, 73, 87; 97, 103, 143, 153, 167; 223, 257
	$5y^2 + 14z^2$	$280x +$ 19, 59, 61, 69, 101; 131, 139, 171, 181, 229; 251, 269
	$2y^2 + 35z^2$	$280x +$ 37, 43, 53, 67, 93; 107, 123, 163, 197, 253; 267, 277.
$t^2 + 78u^2$	$y^2 + 78z^2$	$312x +$ 1, 25, 49, 55, 79; 103, 121, 127, 199, 217; 289, 295
	$2y^2 + 39z^2$	$312x +$ 41, 47, 71, 89, 119; 137, 161, 167, 215, 239; 281, 305
	$3y^2 + 26z^2$	$312x +$ 29, 35, 53, 77, 101; 107, 131, 155, 173, 179; 251, 269
	$6y^2 + 13z^2$	$312x +$ 19, 37, 67, 85, 109; 115, 163, 187, 229, 253; 301, 307.
$t^2 + 86u^2$	$y^2 + 86z^2$ $10y^2 + 4yz + 9z^2$ $6y^2 + 4yz + 15z^2$	$344x +$ 1, 9, 15, 17, 23; 25, 31, 41, 47, 49; 57, 79, 81, 87, 95; 97, 103, 111, 121, 127; 135, 143, 145, 153, 167; 169, 183, 185, 193, 207; 225, 231, 239, 255, 271; 273, 279, 281, 289, 305; 311, 337
	$2y^2 + 43z^2$ $5y^2 + 4yz + 18z^2$ $3y^2 + 4yz + 30z^2$	$344x +$ 3, 5, 19, 27, 29; 37, 45, 51, 61, 69; 75, 77, 85, 91, 93; 115, 123, 125, 131, 141; 147, 149, 155, 157, 163; 171, 179, 205, 211, 227; 235, 237, 243, 245, 261; 277, 285, 291, 309, 323; 331, 333.

Formel.	Quadratische Teiler.	Ungerade lineare Teiler.
$t^2 + 94u^2$	$y^2 + 94z^2$ $2y^2 + 47z^2$ $7y^2 + 4yz + 14z^2$	$376x +$ 1, 7, 9, 17, 25; 49, 55, 63, 65, 71; 79, 81, 89, 95, 97; 103, 111, 119, 121, 143; 145, 153, 159, 169, 175; 177, 183, 191, 209, 215; 225, 239, 241, 247, 249; 263, 271, 289, 303, 319; 335, 337, 343, 345, 353; 361
	$5y^2 + 8yz + 22z^2$ $10y^2 + 8yz + 11z^2$	$376x +$ 5, 11, 13, 19, 29; 35, 43, 45, 67, 69; 77, 85, 91, 93, 99; 107, 109, 117, 123, 125; 133, 139, 163, 171, 179; 181, 187, 203, 211, 219; 221, 227, 229, 245, 261; 275, 293, 301, 315, 317; 323, 325, 339, 349, 355; 373
$t^2 + 102u^2$	$y^2 + 102z^2$	$408x +$ 1, 25, 49, 55, 103; 121, 127, 145, 151, 169; 217, 223, 247, 271, 319; 361
	$6y^2 + 17z^2$	$408x +$ 23, 41, 65, 71, 95; 113, 143, 167, 209, 215; 233, 311, 329, 335, 377; 401
	$2y^2 + 51z^2$	$408x +$ 35, 53, 59, 77, 83; 101, 149, 155, 179, 203; 251, 293, 341, 365, 389; 395
	$3y^2 + 34z^2$	$408x +$ 37, 61, 91, 109, 133; 139, 163, 181, 211, 235; 277, 283, 301, 379, 397; 403.

Tafel VIII.

Enthaltend die trinären quadratischen Teiler der Formel $t^2 + cu^2$ nebst den entsprechenden trinären Werten von c.

Formel.	Trinäre quadratische Teiler.	Trinäre Werte von c.
$t^2 + u^2$	$y^2 + 2yz + 2z^2 = (y+z)^2 + z^2$	1
$t^2 + 2u^2$	$y^2 + 2z^2 = y^2 + z^2 + z^2$	1 + 1
$t^2 + 3u^2$	$2y^2 + 2yz + 2z^2 = (y+z)^2 + y^2 + z^2$	1 + 1 + 1
$t^2 + 5u^2$	$y^2 + 2yz + 6z^2 = (y+z)^2 + z^2 + 4z^2$	4 + 1
$t^2 + 6u^2$	$2y^2 + 3z^2 = (y+z)^2 + (y-z)^2 + z^2$	4 + 1 + 1
$t^2 + 9u^2$	$2y^2 + 2yz + 5z^2 = (y+z)^2 + y^2 + 4z^2$	4 + 4 + 1
$t^2 + 10u^2$	$y^2 + 10z^2 = y^2 + z^2 + 9z^2$	9 + 1
$t^2 + 11u^2$	$2y^2 + 2yz + 6z^2 = (y+2z)^2 + (y-z)^2 + z^2$	9 + 1 + 1
$t^2 + 13u^2$	$y^2 + 13z^2 = y^2 + 4z^2 + 9z^2$	9 + 4
$t^2 + 14u^2$	$3y^2 + 2yz + 5z^2 = y^2 + (y+2z)^2 + (y-z)^2$	9 + 4 + 1
$t^2 + 17u^2$	$y^2 + 17z^2 = y^2 + 16z^2 + z^2$ $2y^2 + 2yz + 9z^2 = (y+2z)^2 + (y-z)^2 + 4z^2$	16 + 1 9 + 4 + 4
$t^2 + 18u^2$	$2y^2 + 9z^2 = (y+2z)^2 + (y-2z)^2 + z^2$	16 + 1 + 1
$t^2 + 19u^2$	$2y^2 + 2yz + 10z^2 = (y+z)^2 + y^2 + 9z^2$	9 + 9 + 1
$t^2 + 21u^2$	$5y^2 + 4yz + 5z^2 = \begin{cases}(2y+z)^2 + y^2 + 4z^2\\(y+2z)^2 + 4y^2 + z^2\end{cases}$	16 + 4 + 1 16 + 4 + 1
$t^2 + 22u^2$	$2y^2 + 11z^2 = (y+z)^2 + (y-z)^2 + 9z^2$	9 + 9 + 4
$t^2 + 25u^2$	$y^2 + 25z^2 = y^2 + 16z^2 + 9z^2$	16 + 9
$t^2 + 26u^2$	$y^2 + 26z^2 = y^2 + z^2 + 25z^2$ $3y^2 + 2yz + 9z^2 = (y+z)^2 + (y-2z)^2 + (y+2z)^2$	25 + 1 16 + 9 + 1
$t^2 + 27u^2$	$2y^2 + 2yz + 14z^2 = (y+3z)^2 + (y-2z)^2 + z^2$	25 + 1 + 1
$t^2 + 29u^2$	$y^2 + 29z^2 = y^2 + 25z^2 + 4z^2$ $5y^2 + 2yz + 6z^2 = (y-z)^2 + (2y+z)^2 + 4z^2$	25 + 4 16 + 9 + 4



Formel.	Trinäre quadratische Teiler.	Trinäre Werte von c.
t^2+30u^2	$5y^2+6z^2=\begin{cases}(y+2z)^2+(2y-z)^2+z^2\\(y-2z)^2+(2y+z)^2+z^2\end{cases}$	$25+4+1$ $25+4+1$
t^2+33u^2	$2y^2+2yz+17z^2=\begin{cases}y^2+(y+z)^2+16z^2\\(y+3z)^2+(y-2z)^2+4z^2\end{cases}$	$16+16+1$ $25+4+4$
t^2+34u^2	$y^2+34z^2=y^2+25z^2+9z^2$ $2y^2+17z^2=(y+2z)^2+(y-2z)^2+9z^2$	$25+9$ $16+9+9$
t^2+35u^2	$6y^2+2yz+6z^2=\begin{cases}(2y+z)^2+(y+z)^2+(y-2z)^2\\(y+2z)^2+(y+z)^2+(2y-z)^2\end{cases}$	$25+9+1$ $25+9+1$
t^2+37u^2	$y^2+37z^2=y^2+36z^2+z^2$	$36+1$
t^2+38u^2	$2y^2+19z^2=(y+3z)^2+(y-3z)^2+z^2$ $3y^2+2yz+13z^2=(y-2z)^2+y^2+(y+3z)^2$	$36+1+1$ $25+9+4$
t^2+41u^2	$y^2+41z^2=y^2+25z^2+16z^2$ $2y^2+2yz+21z^2=(y+2z)^2+(y-z)^2+16z^2$ $5y^2+4yz+9z^2=(2y+2z)^2+(y-2z)^2+z^2$	$25+16$ $16+16+9$ $36+4+1$
t^2+42u^2	$3y^2+14z^2=\begin{cases}(y-2z)^2+(y+3z)^2+(y-z)^2\\(y+2z)^2+(y-3z)^2+(y+z)^2\end{cases}$	$25+16+1$ $25+16+1$
t^2+43u^2	$2y^2+2yz+22z^2=(y+3z)^2+(y-2z)^2+9z^2$	$25+9+9$
t^2+45u^2	$5y^2+9z^2=\begin{cases}(2y+z)^2+(y-2z)^2+4z^2\\(2y-z)^2+(y+2z)^2+4z^2\end{cases}$	$25+16+4$ $25+16+4$
t^2+46u^2	$5y^2+4yz+10z^2=(2y+z)^2+y^2+9z^2$	$36+9+1$
t^2+49u^2	$5y^2+2yz+10z^2=4y^2+(y+z)^2+9z^2$	$36+9+4$
t^2+50u^2	$y^2+50z^2=y^2+49z^2+z^2$ $6y^2+4yz+9z^2=(y+2z)^2+(y-2z)^2+(2y+z)^2$	$49+1$ $25+16+9$
t^2+51u^2	$2y^2+2yz+26z^2=\begin{cases}y^2+(y+z)^2+25z^2\\(y+4z)^2+(y-3z)^2+z^2\end{cases}$	$25+25+1$ $49+1+1$
t^2+53u^2	$y^2+53z^2=y^2+49z^2+4z^2$ $6y^2+2yz+9z^2=(y-2z)^2+(y-z)^2+(2y+2z)^2$	$49+4$ $36+16+1$
t^2+54u^2	$2y^2+27z^2=(y+z)^2+(y-z)^2+25z^2$ $5y^2+2yz+11z^2=(2y-z)^2+(y+3z)^2+z^2$	$25+25+4$ $49+4+1$

Formel.	Trinäre quadratische Teiler.	Trinäre Werte von c.
t^2+57u^2	$2y^2+2yz+29z^2=\begin{cases}(y+4z)^2+(y-3z)^2+4z^2\\(y+3z)^2+(y-2z)^2+16z^2\end{cases}$	$49+4+4$ $25+16+16$
t^2+58u^2	$y^2+58z^2=y^2+49z^2+9z^2$	$49+9$
t^2+59u^2	$2y^2+2yz+30z^2=(y+2z)^2+(y-z)^2+25z^2$ $6y^2+2yz+10z^2=(y+3z)^2+(2y-z)^2+y^2$	$25+25+9$ $49+9+1$
t^2+61u^2	$y^2+61z^2=y^2+36z^2+25z^2$ $5y^2+4yz+13z^2=4y^2+(y+2z)^2+9z^2$	$36+25$ $36+16+9$
t^2+62u^2	$3y^2+2yz+21z^2=(y-z)^2+(y+4z)^2+(y-2z)^2$ $6y^2+4yz+11z^2=(y+z)^2+(y+3z)^2+(2y-z)^2$	$36+25+1$ $59+9+4$
t^2+65u^2	$y^2+65z^2=\begin{cases}y^2+64z^2+z^2\\y^2+49z^2+16z^2\end{cases}$ $9y^2+8yz+9z^2=\begin{cases}(2y-z)^2+(2y+2z)^2+(y+2z)^2\\(y-2z)^2+(2y+2z)^2+(2y+z)^2\end{cases}$	$64+1$ $49+16$ $36+25+4$ $36+25+4$
t^2+66u^2	$2y^2+33z^2=\begin{cases}(y+4z)^2+(y-4z)^2+z^2\\(y+2z)^2+(y-2z)^2+25z^2\end{cases}$ $6y^2+11z^2=\begin{cases}(2y+z)^2+(y-3z)^2+(y+z)^2\\(2y-z)^2+(y+3z)^2+(y-z)^2\end{cases}$	$64+1+1$ $25+25+16$ $49+16+1$ $49+16+1$
t^2+67u^2	$2y^2+2yz+34z^2=(y+4z)^2+(y-3z)^2+9z^2$	$49+9+9$
t^2+69u^2	$5y^2+2yz+14z^2=\begin{cases}(2y+2z)^2+(y-3z)^2+z^2\\(2y-z)^2+(y+3z)^2+4z^2\end{cases}$	$64+4+1$ $49+16+4$
t^2+70u^2	$5y^2+14z^2=\begin{cases}(2y+z)^2+(y-2z)^2+9z^2\\(2y-z)^2+(y+2z)^2+9z^2\end{cases}$	$36+25+9$ $36+25+9$
t^2+73u^2	$y^2+73z^2=y^2+64z^2+9z^2$ $2y^2+2yz+37z^2=(y+z)^2+y^2+36z^2$	$64+9$ $36+36+1$
t^2+74u^2	$y^2+74z^2=y^2+49z^2+25z^2$ $3y^2+2yz+25z^2=(y-3z)^2+y^2+(y+4z)^2$ $9y^2+8yz+10z^2=(2y+3z)^2+(2y-z)^2+y^2$	$49+25$ $49+16+9$ $64+9+1$
t^2+75u^2	$6y^2+6yz+14z^2=\begin{cases}(2y+3z)^2+(y-2z)^2+(y-z)^2\\(2y-z)^2+(y+3z)^2+(y+2z)^2\end{cases}$	$49+25+1$ $49+25+1$

Formel.	Trinäre quadratische Teiler.	Trinäre Werte von c.
t^2+77u^2	$6y^2+2yz+13z^2=\begin{cases}(y+3z)^2+(y-2z)^2+4y^2\\(y-3z)^2+(2y+2z)^2+y^2\end{cases}$	$36+25+16$ $64+9+4$
t^2+78u^2	$3y^2+26z^2=\begin{cases}(y+4z)^2+(y-3z)^2+(y-z)^2\\(y-4z)^2+(y+3z)^2+(y+z)^2\end{cases}$	$49+25+4$ $49+25+4$
t^2+81u^2	$2y^2+2yz+41z^2=(y+4z)^2+(y-3z)^2+16z^2$ $5y^2+4yz+17z^2=(2y+z)^2+y^2+16z^2$	$49+16+16$ $64+16+1$
t^2+82u^2	$y^2+82z^2=y^2+81z^2+z^2$ $2y^2+41z^2=(y+4z)^2+(y-4z)^2+9z^2$	$81+1$ $64+9+9$
t^2+83u^2	$2y^2+2yz+42z^2=(y+5z)^2+(y-4z)^2+z^2$ $6y^2+2yz+14z^2=(2y+z)^2+(y+2z)^2+(y-3z)^2$	$81+1+1$ $49+25+9$
t^2+85u^2	$y^2+85z^2=\begin{cases}y^2+81z^2+4z^2\\y^2+49z^2+36z^2\end{cases}$	$81+4$ $49+36$
t^2+86u^2	$2y^2+43z^2=(y+3z)^2+(y-3z)^2+25z^2$ $3y^2+2yz+29z^2=(y+3z)^2+(y+2z)^2+(y-4z)^2$ $5y^2+4yz+18z^2=(2y-z)^2+(y+4z)^2+z^2$	$36+25+25$ $49+36+1$ $81+4+1$
t^2+89u^2	$y^2+89z^2=y^2+64z^2+25z^2$ $2y^2+2yz+45z^2=(y+5z)^2+(y-4z)^2+4z^2$ $5y^2+2yz+18z^2=(2y+z)^2+(y-z)^2+16z^2$ $9y^2+2yz+10z^2=(2y-z)^2+(y+3z)^2+4y^2$	$64+25$ $81+4+4$ $64+16+9$ $49+36+4$
t^2+90u^2	$9y^2+6yz+11z^2=\begin{cases}(2y+3z)^2+(2y-z)^2+(y-z)^2\\(y+3z)^2+(2y+z)^2+(2y-z)^2\end{cases}$	$64+25+1$ $49+25+16$
t^2+91u^2	$10y^2+6yz+10z^2=\begin{cases}y^2+(3y+z)^2+9z^2\\9y^2+(y+3z)^2+z^2\end{cases}$	$81+9+1$ $81+9+1$
t^2+93u^2	$6y^2+6yz+17z^2=\begin{cases}(y+4z)^2+(y-z)^2+4y^2\\(y-3z)^2+(y+2z)^2+(2y+2z)^2\end{cases}$	$64+25+4$ $64+25+4$
t^2+94u^2	$5y^2+2yz+19z^2=(2y-z)^2+(y+3z)^2+9z^2$ $10y^2+8yz+11z^2=(3y+z)^2+(y+z)^2+9z^2$	$49+36+9$ $81+9+4$
t^2+97u^2	$y^2+97z^2=y^2+81z^2+16z^2$ $2y^2+2yz+49z^2=(y+3z)^2+(y-2z)^2+36z^2$	$81+16$ $36+36+25$

Formel.	Trinäre quadratische Teiler.	Trinäre Werte von c.
$t^2 + 98u^2$	$3y^2 + 2yz + 33z^2 = (y+4z)^2 + (y-4z)^2 + (y+z)^2$ $6y^2 + 4yz + 17z^2 = y^2 + (2y-z)^2 + (y+4z)^2$	64 + 25 + 9 81 + 16 + 1
$t^2 + 99u^2$	$2y^2 + 2yz + 50z^2 = \begin{cases} y^2 + (y+z)^2 + 49z^2 \\ (y+4z)^2 + (y-3z)^2 + 25z^2 \end{cases}$	49 + 49 + 1 49 + 25 + 25
$t^2 + 101u^2$	$y^2 + 101z^2 = y^2 + 100z^2 + z^2$ $5y^2 + 4yz + 21z^2 = (2y-z)^2 + (y+4z)^2 + 4z^2$ $6y^2 + 2yz + 17z^2 = (y+2z)^2 + (y+3z)^2 + (2y-2z)^2$ $9y^2 + 8yz + 13z^2 = (y-2z)^2 + (2y+3z)^2 + 4y^2$	100 + 1 81 + 16 + 4 64 + 36 + 1 49 + 36 + 16
$t^2 + 102u^2$	$2y^2 + 51z^2 = \begin{cases} (y+5z)^2 + (y-5z)^2 + z^2 \\ (y+z)^2 + (y-z)^2 + 49z^2 \end{cases}$	100 + 1 + 1 49 + 49 + 4
$t^2 + 105u^2$	$5y^2 + 21z^2 = \begin{cases} (2y-z)^2 + (y+2z)^2 + 16z^2 \\ (2y+z)^2 + (y-2z)^2 + 16z^2 \\ (2y+2z)^2 + (y-4z)^2 + z^2 \\ (2y-2z)^2 + (y+4z)^2 + z^2 \end{cases}$	64 + 25 + 16 64 + 25 + 16 100 + 4 + 1 100 + 4 + 1
$t^2 + 106u^2$	$y^2 + 106z^2 = y^2 + 81z^2 + 25z^2$ $10y^2 + 4yz + 11z^2 = (y-z)^2 + (3y+z)^2 + 9z^2$	81 + 25 81 + 16 + 9
$t^2 + 107u^2$	$2y^2 + 2yz + 54z^2 = (y+2z)^2 + (y-z)^2 + 49z^2$ $18y^2 + 2yz + 6z^2 = (4y+z)^2 + (y-2z)^2 + (y-z)^2$	49 + 49 + 9 81 + 25 + 1
$t^2 + 109u^2$	$y^2 + 109z^2 = y^2 + 100z^2 + 9z^2$ $5y^2 + 2yz + 22z^2 = (y-3z)^2 + (2y+2z)^2 + 9z^2$	100 + 9 64 + 36 + 9
$t^2 + 110u^2$	$10y^2 + 11z^2 = \begin{cases} (3y+z)^2 + (y-3z)^2 + z^2 \\ (3y-z)^2 + (y+3z)^2 + z^2 \end{cases}$ $6y^2 + 4yz + 19z^2 = \begin{cases} (2y+3z)^2 + (y-3z)^2 + (y-z)^2 \\ (2y+z)^2 + (y+3z)^2 + (y-3z)^2 \end{cases}$	100 + 9 + 1 100 + 9 + 1 81 + 25 + 4 49 + 36 + 25
$t^2 + 113u^2$	$y^2 + 113z^2 = y^2 + 64z^2 + 49z^2$ $2y^2 + 2yz + 57z^2 = (y+5z)^2 + (y-4z)^2 + 16z^2$ $9y^2 + 4yz + 13z^2 = (2y-2z)^2 + (2y+3z)^2 + y^2$	64 + 49 81 + 16 + 16 100 + 9 + 4
$t^2 + 114u^2$	$2y^2 + 57z^2 = \begin{cases} (y+2z)^2 + (y-2z)^2 + 49z^2 \\ (y+4z)^2 + (y-4z)^2 + 25z^2 \end{cases}$ $3y^2 + 38z^2 = \begin{cases} (y+5z)^2 + (y-3z)^2 + (y-2z)^2 \\ (y-5z)^2 + (y+3z)^2 + (y+2z)^2 \end{cases}$	49 + 49 + 16 64 + 25 + 25 64 + 49 + 1 64 + 49 + 1
$t^2 + 115u^2$	$10y^2 + 10yz + 14z^2 = \begin{cases} (3y+z)^2 + (y+2z)^2 + 9z^2 \\ (3y+2z)^2 + (y-z)^2 + 9z^2 \end{cases}$	81 + 25 + 9 81 + 25 + 9

Formel.	Trinäre quadratische Teiler.	Trinäre Werte von c.
t^2+117u^2	$9y^2+6yz+14z^2=\begin{cases}(2y+3z)^2+(2y-2z)^2+(y+z)^2\\(2y+2z)^2+(2y+z)^2+(y-3z)^2\end{cases}$	$100+16+1$ $64+49+4$
t^2+118u^2	$2y^2+59z^2=(y+5z)^2+(y-5z)^2+9z^2$ $11y^2+10yz+13z^2=(y+2z)^2+(y+3z)^2+9y^2$	$100+9+9$ $81+36+4$
t^2+121u^2	$2y^2+2yz+61z^2=(y+4z)^2+(y-3z)^2+36z^2$ $10y^2+6yz+13z^2=(y+3z)^2+9y^2+4z^2$	$49+36+36$ $81+36+4$
t^2+122u^2	$y^2+122z^2=y^2+121z^2+z^2$ $3y^2+2yz+41z^2=(y-4z)^2+(y+5z)^2+y^2$ $9y^2+4yz+14z^2=(2y+3z)^2+(2y-z)^2+(y-2z)^2$	$121+1$ $81+25+16$ $64+49+9$
t^2+123u^2	$2y^2+2yz+62z^2=\begin{cases}(y+3z)^2+(y-2z)^2+49z^2\\(y+6z)^2+(y-5z)^2+z^2\end{cases}$	$49+49+25$ $121+1+1$
t^2+125u^2	$y^2+125z^2=y^2+121z^2+4z^2$ $6y^2+2yz+21z^2=(y+4z)^2+(y+z)^2+(2y-2z)^2$ $9y^2+2yz+14z^2=(2y+z)^2+(2y-2z)^2+(y-3z)^2$	$121+4$ $100+16+9$ $64+36+25$
t^2+126u^2	$5y^2+4yz+26z^2=\begin{cases}(y-4z)^2+(2y+3z)^2+z^2\\y^2+(2y+z)^2+25z^2\end{cases}$	$121+4+1$ $100+25+1$
t^2+129u^2	$2y^2+2yz+65z^2=\begin{cases}y^2+(y+z)^2+64z^2\\(y+6z)^2+(y-5z)^2+4z^2\end{cases}$ $5y^2+2yz+26z^2=\begin{cases}4y^2+(y+z)^2+25z^2\\(2y-z)^2+(y+3z)^2+16z^2\end{cases}$	$64+64+1$ $121+4+4$ $100+25+4$ $64+49+16$
t^2+130u^2	$y^2+130z^2=\begin{cases}y^2+121z^2+9z^2\\y^2+81z^2+49z^2\end{cases}$	$121+9$ $81+49$
t^2+131u^2	$2y^2+2yz+66z^2=(y+5z)^2+(y-4z)^2+25z^2$ $6y^2+2yz+22z^2=(2y+3z)^2+(y-3z)^2+(y-2z)^2$ $10y^2+6yz+14z^2=(3y+2z)^2+(y-3z)^2+z^2$	$81+25+25$ $81+49+1$ $121+9+1$
t^2+133u^2	$13y^2+12yz+13z^2=\begin{cases}(2y+3z)^2+9y^2+4z^2\\(3y+2z)^2+4y^2+9z^2\end{cases}$	$81+36+16$ $81+36+16$
t^2+413^2u	$2y^2+67z^2=(y+3z)^2+(y-3z)^2+49z^2$ $3y^2+2yz+45z^2=(y+2z)^2+(y-5z)^2+(y+4z)^2$ $5y^2+2yz+27z^2=(y-z)^2+(2y+z)^2+25z^2$ $11y^2+6yz+13z^2=(3y+2z)^2+(y-3z)^2+y^2$	$49+49+36$ $81+49+4$ $100+25+9$ $121+9+4$

Formel.	Trinäre quadratische Teiler.	Trinäre Werte von c.
t^2+137u^2	$y^2+137z^2=y^2+121z^2+16z^2$ $2y^2+2yz+69z^2=(y+2z)^2+(y-z)^2+64z^2$ $9y^2+8yz+17z^2=(2y-2z)^2+(2y+3z)^2+(y+2z)^2$	121+16 64+64+9 100+36+1
t^2+138u^2	$11y^2+8yz+14z^2=\begin{cases}(3y+z)^2+(y-2z)^2+(y+3z)^2\\(3y+2z)^2+(y-3z)^2+(y+z)^2\end{cases}$	64+49+25 121+16+1
t^2+139u^2	$2y^2+2yz+70z^2=(y+6z)^2+(y-5z)^2+9z^2$ $10y^2+2yz+14z^2=(3y+z)^2+(y-2z)^2+9z^2$	121+9+9 81+49+9
t^2+141u^2	$5y^2+4yz+29z^2=\begin{cases}(2y+3z)^2+(y-4z)^2+4z^2\\4y^2+(y+2z)^2+25z^2\end{cases}$	121+16+4 100+25+16
t^2+142u^2	$11y^2+2yz+13z^2=9y^2+(y-2z)^2+(y+3z)^2$	81+36+25
t^2+145u^2	$y^2+145z^2=\begin{cases}y^2+144z^2+z^2\\y^2+81z^2+64z^2\end{cases}$ $5y^2+29z^2=\begin{cases}(y+4z)^2+(2y-2z)^2+9z^2\\(y-4z)^2+(2y+2z)^2+9z^2\end{cases}$	144+1 81+64 100+36+9 100+36+9
t^2+146u^2	$y^2+146z^2=y^2+121z^2+25z^2$ $2y^2+73z^2=(y+6z)^2+(y-6z)^2+z^2$ $3y^2+2yz+49z^2=(y-3z)^2+(y-2z)^2+(y+6z)^2$ $6y^2+4yz+25z^2=y^2+(2y+3z)^2+(y-4z)^2$ $9y^2+8yz+18z^2=(2y+z)^2+(2y-z)^2+(y+4z)^2$	121+25 144+1+1 81+64+1 121+16+9 81+49+16
t^2+147u^2	$6y^2+6yz+26z^2=\begin{cases}(y+z)^2+(y-4z)^2+(2y+3z)^2\\(2y-z)^2+(y+5z)^2+y^2\end{cases}$	121+25+1 121+25+1
t^2+149u^2	$y^2+149z^2=y^2+100z^2+49z^2$ $5y^2+2yz+30z^2=(y+5z)^2+(2y-2z)^2+z^2$ $6y^2+2yz+25z^2=(y+4z)^2+(y-3z)^2+4y^2$ $9y^2+4yz+17z^2=4y^2+(2y-z)^2+(y+4z)^2$	100+49 144+4+1 64+49+36 81+64+4
t^2+150u^2	$11y^2+4yz+14z^2=\begin{cases}(3y+2z)^2+(y-z)^2+(y-3z)^2\\(3y-z)^2+(y+3z)^2+(y+2z)^2\end{cases}$	121+25+4 100+49+1
t^2+153u^2	$2y^2+2yz+77z^2=\begin{cases}(y+3z)^2+(y-2z)^2+64z^2\\(y+6z)^2+(y-5z)^2+16z^2\end{cases}$ $9y^2+17z^2=\begin{cases}(2y+3z)^2+(2y-2z)^2+(y-2z)^2\\(2y+2z)^2+(2y-3z)^2+(y+2z)^2\end{cases}$	64+64+25 121+16+16 100+49+4 100+49+4

Formel.	Trinäre quadratische Teiler.	Trinäre Werte von c.
t^2+154u^2	$10y^2+8yz+17z^2=\begin{cases}(y+4z)^2+9y^2+z^2\\(y-2z)^2+(3y+2z)^2+9z^2\end{cases}$	$144+9+1$ $81+64+9$
t^2+155u^2	$6y^2+2yz+26z^2=\begin{cases}(2y+3z)^2+(y-4z)^2+(y-z)^2\\(2y+z)^2+(y+3z)^2+(y-4z)^2\end{cases}$	$121+25+9$ $81+49+25$
t^2+157u^2	$y^2+157z^2=y^2+121z^2+36z^2$ $13y^2+10yz+14z^2=(3y+3z)^2+(2y-2z)^2+z^2$	$121+36$ $144+9+4$
t^2+158u^2	$3y^2+2yz+53z^2=(y-4z)^2+(y+6z)^2+(y-z)^2$ $6y^2+4yz+27z^2=(2y-z)^2+(y+5z)^2+(y-z)^2$	$100+49+9$ $121+36+1$
t^2+161u^2	$5y^2+4yz+33z^2=\begin{cases}(2y+2z)^2+(y-2z)^2+25z^2\\(2y-z)^2+(y+4z)^2+16z^2\end{cases}$ $10y^2+6yz+17z^2=\begin{cases}y^2+(3y+z)^2+16z^2\\(3y+2z)^2+(y-3z)^2+4z^2\end{cases}$	$100+36+25$ $81+64+16$ $144+16+1$ $121+36+4$
t^2+162u^2	$2y^2+81z^2=(y+4z)^2+(y-4z)^2+49z^2$ $11y^2+10yz+17z^2=(y+2z)^2+(3y+2z)^2+(y-3z)^2$	$64+49+49$ $121+25+16$
t^2+163u^2	$2y^2+2yz+82z^2=y^2+(y+z)^2+81z^2$	$81+81+1$
t^2+165u^2	$6y^2+6yz+29z^2=\begin{cases}(y+5z)^2+(y-2z)^2+4y^2\\(y+3z)^2+(y-4z)^2+(2y+2z)^2\\(2y+4z)^2+(y-3z)^2+(y-2z)^2\\(y+4z)^2+(y+3z)^2+(2y-2z)^2\end{cases}$	$100+49+16$ $100+49+16$ $100+64+1$ $100+64+1$
t^2+166u^2	$2y^2+83z^2=(y+z)^2+(y-z)^2+81z^2$ $5y^2+4yz+34z^2=(2y+3z)^2+(y-4z)^2+9z^2$ $13y^2+8yz+14z^2=(3y+2z)^2+(2y-z)^2+9z^2$	$81+81+4$ $121+36+9$ $81+49+36$
t^2+169u^2	$y^2+169z^2=y^2+144z^2+25z^2$ $10y^2+2yz+17z^2=(y+z)^2+9y^2+16z^2$	$144+25$ $144+16+9$
t^2+170u^2	$y^2+170z^2=\begin{cases}y^2+169z^2+z^2\\y^2+121z^2+49z^2\end{cases}$ $9y^2+2yz+19z^2=\begin{cases}(2y+3z)^2+(2y-3z)^2+(y+z)^2\\(2y-z)^2+(2y+3z)^2+(y-3z)^2\end{cases}$	$169+1$ $121+49$ $144+25+1$ $81+64+25$
t^2+171u^2	$2y^2+2yz+86z^2=\begin{cases}(y+6z)^2+(y-5z)^2+25z^2\\(y+7z)^2+(y-6z)^2+z^2\end{cases}$ $14y^2+10yz+14z^2=\begin{cases}(3y+2z)^2+(2y+z)^2+(y-3z)^2\\(3y-z)^2+(y+2z)^2+(2y+3z)^2\end{cases}$	$121+25+25$ $169+1+1$ $121+49+1$ $121+49+1$

Formel.	Trinäre quadratische Teiler.	Trinäre Werte von c.
t^2+173u^2	$y^2+173z^2=y^2+169z^2+4z^2$ $6y^2+2yz+29z^2=y^2+(y+5z)^2+(2y-2z)^2$ $9y^2+8yz+21z^2=(2y-z)^2+(y-2z)^2+(2y+4z)^2$ $13y^2+6yz+14z^2=(3y-z)^2+(2y+3z)^2+4z^2$	$169+4$ $144+25+4$ $100+64+9$ $121+36+16$
t^2+174u^2	$6y^2+29z^2=\begin{cases}(y-4z)^2+(2y+3z)^2+(y-2z)^2\\(y+4z)^2+(2y-3z)^2+(y+2z)^2\end{cases}$ $5y^2+2yz+35z^2=\begin{cases}(y+3z)^2+(2y-z)^2+25z^2\\(2y+3z)^2+(y-5z)^2+z^2\end{cases}$	$121+49+4$ $121+49+4$ $100+49+25$ $169+4+1$
t^2+177u^2	$2y^2+2yz+89z^2=\begin{cases}(y+4z)^2+(y-3z)^2+64z^2\\(y+7z)^2+(y-6z)^2+4z^2\end{cases}$	$64+64+49$ $169+4+4$
t^2+178u^2	$y^2+178z^2=y^2+169z^2+9z^2$ $2y^2+89z^2=(y+2z)^2+(y-2z)^2+81z^2$ $11y^2+6yz+17z^2=9y^2+(y+4z)^2+(y-z)^2$	$169+9$ $81+81+16$ $144+25+9$
t^2+179u^2	$2y^2+2yz+90z^2=(y+5z)^2+(y-4z)^2+49z^2$ $6y^2+2yz+30z^2=(2y-z)^2+(y-2z)^2+(y+5z)^2$ $10y^2+2yz+18z^2=(3y-z)^2+(y+4z)^2+z^2$	$81+49+49$ $121+49+9$ $169+9+1$
t^2+181u^2	$y^2+181z^2=y^2+100z^2+81z^2$ $5y^2+4yz+37z^2=(2y+z)^2+y^2+36z^2$ $13y^2+2yz+14z^2=(3y-z)^2+(2y+2z)^2+9z^2$	$100+81$ $144+36+1$ $81+64+36$
t^2+182u^2	$13y^2+14z^2=\begin{cases}(3y+2z)^2+(2y-3z)^2+z^2\\(3y-2z)^2+(2y+3z)^2+z^2\end{cases}$ $3y^2+2yz+61z^2=\begin{cases}(y-6z)^2+(y+4z)^2+(y+3z)^2\\(y-5z)^2+(y+6z)^2+y^2\end{cases}$	$169+9+4$ $169+9+4$ $100+81+1$ $121+36+25$
t^2+185u^2	$y^2+185z^2=\begin{cases}y^2+169z^2+16z^2\\y^2+121z^2+64z^2\end{cases}$ $9y^2+4yz+21z^2=\begin{cases}(2y+z)^2+(2y+2z)^2+(y-4z)^2\\(2y-2z)^2+(2y+z)^2+(y+4z)^2\end{cases}$	$169+16$ $121+64$ $100+81+4$ $100+49+36$
t^2+186u^2	$3y^2+62z^2=\begin{cases}(y-z)^2+(y+6z)^2+(y-5z)^2\\y+z)^2+(y-6z)^2+(y+5z)^2\end{cases}$ $11y^2+2yz+17z^2=\begin{cases}y^2+(y+4z)^2+(3y-z)^2\\(3y+2z)^2+(y-3z)^2+(y-2z)^2\end{cases}$	$121+49+16$ $121+49+16$ $169+16+1$ $121+64+1$

Formel.	Trinäre quadratische Teiler.	Trinäre Werte von c.
t^2+187u^2	$2y^2+2yz+94z^2=\begin{cases}(y+3z)^2+(y-2z)^2+81z^2\\(y+7z)^2+(y-6z)^2+9z^2\end{cases}$	81 + 81 + 25 169 + 9 + 9
t^2+189u^2	$5y^2+2yz+38z^2=\begin{cases}(2y+3z)^2+(y-5z)^2+4z^2\\(2y+2z)^2+(y-3z)^2+25z^2\end{cases}$ $14y^2+14yz+17z^2=\begin{cases}(y+4z)^2+(3y+z)^2+4y^2\\(y-3z)^2+(3y+2z)^2+(2y+2z)^2\end{cases}$	169 + 16 + 4 100 + 64 + 25 121 + 64 + 4 121 + 64 + 4
t^2+190u^2	$10y^2+19z^2=\begin{cases}(3y+z)^2+(y-3z)^2+9z^2\\(3y-z)^2+(y+3z)^2+9z^2\end{cases}$	100 + 81 + 9 100 + 81 + 9
t^2+193u^2	$y^2+193z^2=y^2+144z^2+49z^2$ $2y^2+2yz+97z^2=(y+6z)^2+(y-5z)^2+36z^2$	144 + 49 121 + 36 + 36
t^2+194u^2	$y^2+194z^2=y^2+169z^2+25z^2$ $2y^2+97z^2=(y+6z)^2+(y-6z)^2+25z^2$ $3y^2+2yz+65z^2=(y-6z)^2+(y+5z)^2+(y+2z)^2$ $6y^2+4yz+33z^2=(2y+z)^2+(y+4z)^2+(y-4z)^2$ $9y^2+4yz+22z^2=(2y+3z)^2+(2y-3z)^2+(y+2z)^2$ $11y^2+4yz+18z^2=(y+4z)^2+(3y-z)^2+(y+z)^2$	169 + 25 144 + 25 + 25 121 + 64 + 9 81 + 64 + 49 144 + 49 + 1 169 + 16 + 9
t^2+195u^2	$14y^2+2yz+14z^2=\begin{cases}(3y+2z)^2+(2y-3z)^2+(y+z)^2\\(3y-2z)^2+(2y+3z)^2+(y+z)^2\\(3y+2z)^2+(2y-z)^2+(y-3z)^2\\(3y-z)^2+(2y+3z)^2+(y-2z)^2\end{cases}$	169 + 25 + 1 169 + 25 + 1 121 + 49 + 25 121 + 49 + 25
t^2+197u^2	$y^2+197z^2=y^2+196z^2+z^2$ $6y^2+2yz+33z^2=(y-5z)^2+(y+2z)^2+(2y+2z)^2$ $9y^2+2yz+22z^2=(2y+2z)^2+(2y-3z)^2+(y+3z)^2$	196 + 1 144 + 49 + 4 100 + 81 + 16
t^2+198u^2	$2y^2+99z^2=\begin{cases}(y+7z)^2+(y-7z)^2+z^2\\(y+5z)^2+(y-5z)^2+49z^2\end{cases}$	196 + 1 + 1 100 + 49 + 49
t^2+201u^2	$2y^2+2yz+101z^2=\begin{cases}y^2+(y+z)^2+100z^2\\(y+7z)^2+(y-6z)^2+16z^2\end{cases}$ $5y^2+4yz+41z^2=\begin{cases}(2y-2z)^2+(y+6z)^2+z^2\\(2y+3z)^2+(y-4z)^2+16z^2\end{cases}$	100 + 100 + 1 169 + 16 + 16 196 + 4 + 1 121 + 64 + 16

Formel.	Trinäre quadratische Teiler.	Trinäre Werte von c.
t^2+202u^2	$y^2+202z^2=y^2+121z^2+81z^2$ $14y^2+12yz+17z^2=(y+4z)^2+(2y+z)^2+9y^2$	$121+81$ $144+49+9$
t^2+203u^2	$6y^2+2yz+34z^2=\begin{cases}(2y+3z)^2+(y-5z)^2+y^2\\(2y-3z)^2+(y+4z)^2+(y+3z)^2\end{cases}$	$169+25+9$ $121+81+1$
t^2+205u^2	$y^2+205z^2=\begin{cases}y^2+196z^2+9z^2\\y^2+169z^2+36z^2\end{cases}$ $5y^2+41z^2=\begin{cases}(2y+z)^2+(y-2z)^2+36z^2\\(2y-z)^2+(y+2z)^2+36z^2\end{cases}$	$196+9$ $169+36$ $144+36+25$ $144+36+25$
t^2+206u^2	$3y^2+2yz+69z^2=(y-4z)^2+(y-2z)^2+(y+7z)^2$ $5y^2+4yz+42z^2=(2y-z)^2+(y+4z)^2+25z^2$ $6y^2+4yz+35z^2=(2y+3z)^2+(y+z)^2+(y-5z)^2$ $10y^2+4yz+21z^2=(3y+2z)^2+(y-4z)^2+z^2$ $11y^2+10yz+21z^2=(3y+z)^2+(y+4z)^2+(y-2z)^2$	$121+81+4$ $100+81+25$ $169+36+1$ $196+9+1$ $121+49+36$
t^2+209u^2	$2y^2+2yz+105z^2=\begin{cases}(y+2z)^2+(y-z)^2+100z^2\\(y+5z)^2+(y-4z)^2+64z^2\end{cases}$ $10y^2+2yz+21z^2=\begin{cases}(3y-z)^2+(y+4z)^2+4z^2\\(3y+z)^2+(y-2z)^2+16z^2\end{cases}$ $13y^2+10yz+18z^2=\begin{cases}(3y+z)^2+(2y+z)^2+16z^2\\(3y-z)^2+(2y+4z)^2+z^2\end{cases}$	$100+100+9$ $81+64+64$ $169+36+4$ $144+49+16$ $144+64+1$ $196+9+4$
t^2+210u^2	$6y^2+35z^2=\begin{cases}(y+5z)^2+(2y-3z)^2+(y+z)^2\\(y-5z)^2+(2y+3z)^2+(y-z)^2\\(y+5z)^2+(y-3z)^2+(2y-z)^2\\(y-5z)^2+(y+3z)^2+(2y+z)^2\end{cases}$	$169+25+16$ $169+25+16$ $121+64+25$ $121+64+25$
t^2+211u^2	$2y^2+2yz+106z^2=(y+4z)^2+(y-3z)^2+81z^2$ $10y^2+6yz+22z^2=(3y+2z)^2+(y-3z)^2+9z^2$	$81+81+49$ $121+81+9$
t^2+213u^2	$14y^2+10yz+17z^2=\begin{cases}(2y+4z)^2+(3y-z)^2+y^2\\(3y+2z)^2+(2y-2z)^2+(y+3z)^2\end{cases}$	$196+16+1$ $100+64+49$
t^2+214u^2	$2y^2+107z^2=(y+7z)^2+(y-7z)^2+9z^2$ $5y^2+2yz+43z^2=(2y+3z)^2+(y-5z)^2+9z^2$	$196+9+9$ $169+36+9$

Formel.	Trinäre quadratische Teiler.	Trinäre Werte von c.
$t^2 + 217u^2$	$13y^2 + 4yz + 17z^2 = \begin{cases} (3y + 2z)^2 + (2y - 2z)^2 + 9z^2 \\ 9y^2 + (2y + z)^2 + 16z^2 \end{cases}$	100 + 81 + 36
$t^2 + 218u^2$	$y^2 + 218z^2 = y^2 + 169z^2 + 49z^2$ $3y^2 + 2yz + 73z^2 = (y + 6z)^2 + (y - 6z)^2 + (y + z)^2$ $9y^2 + 8yz + 26z^2 = (2y + 3z)^2 + (2y + z)^2 + (y - 4z)^2$	169 + 49 144 + 49 + 25 121 + 81 + 16
$t^2 + 219u^2$	$2y^2 + 2yz + 110z^2 = \begin{cases} (y + 6z)^2 + (y - 5z)^2 + 49z^2 \\ (y + 7z)^2 + (y - 6z)^2 + 25z^2 \end{cases}$ $38y^2 + 6yz + 6z^2 = \begin{cases} (6y + z)^2 + (y - z)^2 + (y - 2z)^2 \\ (5y - z)^2 + (2y + z)^2 + (3y + 2z)^2 \end{cases}$	121 + 49 + 49 169 + 25 + 25 169 + 49 + 1 169 + 49 + 1
$t^2 + 221u^2$	$y^2 + 221z^2 = \begin{cases} y^2 + 196z^2 + 25z^2 \\ y^2 + 121z^2 + 100z^2 \end{cases}$ $9y^2 + 4yz + 25z^2 = \begin{cases} (2y + 4z)^2 + (2y - 3z)^2 + y^2 \\ (2y + 3z)^2 + (y - 4z)^2 + 4y^2 \end{cases}$ $13y^2 + 17z^2 = \begin{cases} (3y + 2z)^2 + (2y - 3z)^2 + 4z^2 \\ (3y - 2z)^2 + (2y + 3z)^2 + 4z^2 \end{cases}$	196 + 25 121 + 100 196 + 16 + 9 121 + 64 + 36 169 + 36 + 16 169 + 36 + 16
$t^2 + 222u^2$	$11y^2 + 6yz + 21z^2 = \begin{cases} (3y + 2z)^2 + (y - 4z)^2 + (y + z)^2 \\ (3y - z)^2 + (y + 4z)^2 + (y + 2z)^2 \end{cases}$ $3y^2 + 74z^2 = \begin{cases} (y + 7z)^2 + (y - 4z)^2 + (y - 3z)^2 \\ (y - 7z)^2 + (y + 4z)^2 + (y + 3z)^2 \end{cases}$	196 + 25 + 1 169 + 49 + 4 121 + 100 + 1 121 + 100 + 1
$t^2 + 225u^2$	$26y^2 + 6yz + 9z^2 = \begin{cases} (4y + 2z)^2 + (3y - 2z)^2 + (y + z)^2 \\ (5y + z)^2 + (y - 2z)^2 + 4z^2 \end{cases}$	196 + 25 + 4 121 + 100 + 4
$t^2 + 226u^2$	$y^2 + 226z^2 = y^2 + 225z^2 + z^2$ $2y^2 + 113z^2 = (y + 4z)^2 + (y - 4z)^2 + 81z^2$ $11y^2 + 8yz + 22z^2 = (y - 2z)^2 + (y - 3z)^2 + (3y + 3z)^2$	225 + 1 81 + 81 + 64 144 + 81 + 1
$t^2 + 227u^2$	$2y^2 + 2yz + 114z^2 = (y + 8z)^2 + (y - 7z)^2 + z^2$ $6y^2 + 2yz + 38z^2 = (y + 5z)^2 + (y + 2z)^2 + (2y - 3z)^2$ $18y^2 + 10yz + 14z^2 = (y + 3z)^2 + (y - 2z)^2 + (4y + z)^2$	225 + 1 + 1 169 + 49 + 9 121 + 81 + 25

Formel.	Trinäre quadratische Teiler.	Trinäre Werte von c.
t^2+229u^2	$y^2+229z^2=y^2+225z^2+4z^2$	225 + 4
	$5y^2+2yz+46z^2=(y+3z)^2+(2y-z)^2+36z^2$	144 + 49 + 36
	$17y^2+6yz+14z^2=(2y-z)^2+(2y-2z)^2+(3y+3z)^2$	144 + 81 + 4
t^2+230u^2	$5y^2+46z^2=\begin{cases}(y+6z)^2+(2y-3z)^2+z^2\\(y-6z)^2+(2y+3z)^2+z^2\end{cases}$	225 + 4 + 1 225 + 4 + 1
	$14y^2+12yz+19z^2=\begin{cases}(y+3z)^2+(2y+3z)^2+(3y-z)^2\\(y-3z)^2+(2y+3z)^2+(3y+z)^2\end{cases}$	121 + 100 + 9 100 + 81 + 49
	$21y^2+2yz+11z^2=\begin{cases}(y-z)^2+(4y-z)^2+(2y+3z)^2\\(2y+z)^2+(y+3z)^2+(4y-z)^2\end{cases}$	196 + 25 + 9 169 + 36 + 25
t^2+233u^2	$y^2+233z^2=y^2+169z^2+64z^2$	169 + 64
	$2y^2+2yz+117z^2=(y+8z)^2+(y-7z)^2+4z^2$	225 + 4 + 4
	$26y^2+2yz+9z^2=(y-z)^2+(3y-2z)^2+(4y+2z)^2$	196 + 36 + 1
	$18y^2+2yz+13z^2=(y-2z)^2+(y+3z)^2+16y^2$	144 + 64 + 25
t^2+234u^2	$26y^2+9z^2=\begin{cases}(3y-2z)^2+(4y+z)^2+(y+2z)^2\\(3y+2z)^2+(4y-z)^2+(y-2z)^2\end{cases}$	121 + 64 + 49 121 + 64 + 49
	$17y^2+4yz+14z^2=\begin{cases}(2y+z)^2+(3y+2z)^2+(2y-3z)^2\\(2y+z)^2+(3y-2z)^2+(2y+3z)^2\end{cases}$	169 + 64 + 1 169 + 49 + 16
t^2+235u^2	$10y^2+10yz+26z^2=\begin{cases}(y-4z)^2+(3y+3z)^2+z^2\\(y+5z)^2+9y^2+z^2\end{cases}$	225 + 9 + 1 225 + 9 + 1
t^2+237u^2	$6y^2+6yz+41z^2=\begin{cases}y^2+(2y+4z)^2+(y-5z)^2\\(y+z)^2+(2y-2z)^2+(y+6z)^2\end{cases}$	196 + 25 + 16 196 + 25 + 16
	$14y^2+2yz+17z^2=\begin{cases}4y^2+(3y-z)^2+(y+4z)^2\\(2y+2z)^2+(3y-2z)^2+(y+3z)^2\end{cases}$	169 + 64 + 4 121 + 100 + 16
t^2+238u^2	$13y^2+6yz+19z^2=\begin{cases}(3y+3z)^2+(2y-3z)^2+z^2\\(3y-z)^2+(2y+3z)^2+9z^2\end{cases}$	225 + 9 + 4 121 + 81 + 36
t^2+241u^2	$y^2+241z^2=y^2+225z^2+16z^2$	225 + 16
	$2y^2+2yz+121z^2=(y+7z)^2+(y-6z)^2+36z^2$	169 + 36 + 36
	$5y^2+4yz+49z^2=(y+6z)^2+(2y-2z)^2+9z^2$	196 + 36 + 9
	$10y^2+6yz+25z^2=9y^2+(y+3z)^2+16z^2$	144 + 81 + 16

Formel.	Trinäre quadratische Teiler.	Trinäre Werte von c.
t^2+242u^2	$2y^2+121z^2=(y+6z)^2+(y-6z)^2+49z^2$ $6y^2+4yz+41z^2=(y+6z)^2+(y-2z)^2+(2y-z)^2$ $17y^2+16yz+18z^2=(4y+z)^2+(y+4z)^2+z^2$	$144+49+49$ $169+64+9$ $225+16+1$
t^2+243u^2	$2y^2+2yz+122z^2=y^2+(y+z)^2+121z^2$ $14y^2+6yz+18z^2=(y+4z)^2+(3y-z)^2+(2y+z)^2$	$121+121+1$ $169+49+25$
t^2+245u^2	$5y^2+49z^2=\begin{cases}(2y+3z)^2+(y-6z)^2+4z^2\\(2y-3z)^2+(y+6z)^2+4z^2\end{cases}$ $6y^2+2yz+41z^2=\begin{cases}(y-3z)^2+(y-4z)^2+(2y+4z)^2\\(y+5z)^2+(y-4z)^2+4y^2\end{cases}$	$225+16+4$ $225+16+4$ $144+100+1$ $100+81+64$
t^2+246u^2	$2y^2+123z^2=\begin{cases}(y+z)^2+(y-z)^2+121z^2\\(y+7z)^2+(y-7z)^2+25z^2\end{cases}$ $5y^2+4yz+50z^2=\begin{cases}(2y+3z)^2+(y-4z)^2+25z^2\\(2y+z)^2+y^2+49z^2\end{cases}$	$121+121+4$ $196+25+25$ $121+100+25$ $196+49+1$
t^2+249u^2	$2y^2+2yz+125z^2=\begin{cases}(y+4z)^2+(y-3z)^2+100z^2\\(y+6z)^2+(y-5z)^2+64z^2\end{cases}$	$100+100+49$ $121+64+64$
t^2+250u^2	$y^2+250z^2=y^2+169z^2+81z^2$ $11y^2+10yz+25z^2=(y-4z)^2+y^2+(3y+3z)^2$	$169+81$ $225+16+9$
t^2+251u^2	$2y^2+2yz+126z^2=(y-z)^2+(y+2z)^2+121z^2$ $6y^2+2yz+42z^2=(2y+z)^2+(y-5z)^2+(y+4z)^2$ $14y^2+2yz+18z^2=(3y+z)^2+(2y+z)^2+(y-4z)^2$ $10y^2+6yz+26z^2=(3y+z)^2+y^2+25z^2$	$121+121+9$ $121+81+49$ $169+81+1$ $225+25+1$
u. s. w.	u. s. w.	u. s. w.
t^2+403u^2	$22y^2+18yz+22z^2=\begin{cases}(2y+3z)^2+(3y+3z)^2+(3y-2z)^2\\(3y+2z)^2+(3y+3z)^2+(2y-3z)^2\end{cases}$	$225+169+9$ $225+169+9$
u. s. w.	u. s. w.	u. s. w.

Tafel IX.

Werte des Produkts $\frac{2}{3} \cdot \frac{4}{5} \cdot \frac{6}{7} \cdot \frac{10}{11} \cdots \frac{\omega - 1}{\omega}$.

ω.	Produkt.	ω.	Produkt.	ω.	Produkt.	ω.	Produkt.	ω.	Produkt.
3	0.666667	181	0.212108	421	0.184357	673	0.171189	953	0.162925
5	0.533333	191	0.210998	431	0.183929	677	0.170936	967	0.162757
7	0.457143	193	0.209904	433	0.183505	683	0.170686	971	0.162589
11	0.415584	197	0.208839	439	0.183087	691	0.170439	977	0.162423
13	0.383616	199	0.207789	443	0.182673	701	0.170196	983	0.162257
17	0.361051	211	0.206804	449	0.182266	709	0.169956	991	0.162093
19	0.342048	223	0.205877	457	0.181868	719	0.169720	997	0.161930
23	0.327176	227	0.204970	461	0.181473	727	0.169486	1009	0.161770
29	0.315894	229	0.204075	463	0.181081	733	0.169255	1013	0.161610
31	0.305704	233	0.203199	467	0.180693	739	0.169026	1019	0.161451
37	0.297442	239	0.202349	479	0.180316	743	0.168799	1021	0.161293
41	0.290187	241	0.201509	487	0.179946	751	0.168574	1031	0.161137
43	0.283439	251	0.200707	491	0.179579	757	0.168351	1033	0.160981
47	0.277408	257	0.199926	499	0.179220	761	0.168130	1039	0.160826
53	0.272174	263	0.199165	503	0.178863	769	0.167911	1049	0.160673
59	0.267561	269	0.198425	509	0.178512	773	0.167694	1051	0.160520
61	0.263175	271	0.197693	521	0.178169	787	0.167481	1061	0.160369
67	0.259247	277	0.196979	523	0.177829	797	0.167271	1063	0.160218
71	0.255595	281	0.196278	541	0.177500	809	0.167064	1069	0.160068
73	0.252094	283	0.195585	547	0.177175	811	0.166858	1087	0.159921
79	0.248903	293	0.194917	557	0.176857	821	0.166655	1091	0.159774
83	0.245904	307	0.194282	563	0.176543	823	0.166453	1093	0.159628
89	0.243141	311	0.193657	569	0.176233	827	0.166252	1097	0.159482
97	0.240635	313	0.193039	571	0.175924	829	0.166051	1103	0.159337
101	0.238252	317	0.192430	577	0.175619	839	0.165852	1109	0.159193
103	0.235939	331	0.191848	587	0.175320	853	0.165658	1117	0.159051
107	0.233734	337	0.191279	593	0.175025	857	0.165465	1123	0.158909
109	0.231590	347	0.190728	599	0.174732	859	0.165272	1129	0.158768
113	0.229540	349	0.190181	601	0.174442	863	0.165081	1151	0.158630
127	0.227733	353	0.189643	607	0.174154	877	0.164892	1153	0.158492
131	0.225994	359	0.189114	613	0.173870	881	0.164705	1163	0.158356
137	0.224345	367	0.188599	617	0.173588	883	0.164518	1171	0.158221
139	0.222731	373	0.188093	619	0.173308	887	0.164332	1181	0.158087
149	0.221236	379	0.187597	631	0.173033	907	0.164151	1187	0.157954
151	0.219771	383	0.187107	641	0.172763	911	0.163972	1193	0.157822
157	0.218371	389	0.186626	643	0.172495	919	0.163794	1201	0.157691
163	0.217031	397	0.186156	647	0.172228	929	0.163618	1213	0.157561
167	0.215732	401	0.185692	653	0.171964	937	0.163443	1217	0.157432
173	0.214485	409	0.185238	659	0.171703	941	0.163269	1223	0.157303
179	0.213286	419	0.184796	661	0.171444	947	0.163096	1229	0.157175

Tafel X.

Kleinste der Gleichung $x^2 - Ny^2 = \pm 1$ genügende Werte von x und y für jede nichtquadratische Zahl N von 2 bis 1003.

N	$x : y$	N	$x : y$
2	1 : 1	45	161 : 24
3	2 : 1	46	24335 : 3588
5	2 : 1	47	48 : 7
6	5 : 2	48	7 : 1
7	8 : 3	50	7 : 1
8	3 : 1	51	50 : 7
10	3 : 1	52	649 : 90
11	10 : 3	53	182 : 25
12	7 : 2	54	485 : 66
13	18 : 5	55	89 : 12
14	15 : 4	56	15 : 2
15	4 : 1	57	151 : 20
17	4 : 1	58	99 : 13
18	17 : 4	59	530 : 69
19	170 : 39	60	31 : 4
20	9 : 2	61	29718 : 3805
21	55 : 12	62	63 : 8
22	197 : 42	63	8 : 1
23	24 : 5	65	8 : 1
24	5 : 1	66	65 : 8
26	5 : 1	67	48842 : 5967
27	26 : 5	68	33 : 4
28	127 : 24	69	7775 : 936
29	70 : 13	70	251 : 30
30	11 : 2	71	3480 : 413
31	1520 : 273	72	17 : 2
32	17 : 3	73	1068 : 125
33	23 : 4	74	43 : 5
34	35 : 6	75	26 : 3
35	6 : 1	76	57799 : 6630
37	6 : 1	77	351 : 40
38	37 : 6	78	53 : 6
39	25 : 4	79	80 : 9
40	19 : 3	80	9 : 1
41	32 : 5	82	9 : 1
42	13 : 2	83	82 : 9
43	3482 : 531	84	55 : 6
44	199 : 30	85	378 : 41

N	$x : y$	N	$x : y$
86	10405 : 1122	132	23 : 2
87	28 : 3	133	2588599 : 224460
88	197 : 21	134	145925 : 12606
89	500 : 53	135	244 : 21
90	19 : 2	136	35 : 3
91	1574 : 165	137	1744 : 149
92	1151 : 120	138	47 : 4
93	12151 : 1260	139	77563250 : 6578829
94	2143295 : 221064	140	71 : 6
95	39 : 4	141	95 : 8
96	49 : 5	142	143 : 12
97	5604 : 569	143	12 : 1
98	99 : 10	145	12 : 1
99	10 : 1	146	145 : 12
101	10 : 1	147	97 : 8
102	101 : 10	148	73 : 6
103	227528 : 22419	149	113582 : 9305
104	51 : 5	150	49 : 4
105	41 : 4	151	1728148040 : 140634693
106	4005 : 389	152	37 : 3
107	962 : 93	153	2177 : 176
108	1351 : 130	154	21295 : 1716
109	8890182 : 851525	155	249 : 20
110	21 : 2	156	25 : 2
111	295 : 28	157	4832118 : 385645
112	127 : 12	158	7743 : 616
113	776 : 73	159	1324 : 105
114	1025 : 96	160	721 : 57
115	1126 : 105	161	11775 : 928
116	9801 : 910	162	19601 : 1540
117	649 : 60	163	64080026 : 5019135
118	306917 : 28254	164	2049 : 160
119	120 : 11	165	1079 : 84
120	11 : 1	166	1700902565 : 132015642
122	11 : 1	167	168 : 13
123	122 : 11	168	13 : 1
124	4620799 : 414960	170	13 : 1
125	682 : 61	171	170 : 13
126	449 : 40	172	24248647 : 1848942
127	4730624 : 419775	173	1118 : 85
128	577 : 51	174	1451 : 110
129	16855 : 1484	175	2024 : 153
130	57 : 5	176	199 : 15
131	10610 : 927	177	62423 : 4692

N	$x:y$	N	$x:y$
178	1601 : 120	223	224 : 15
179	4190210 : 313191	224	15 : 1
180	161 : 12	226	15 : 1
181	1111225770 : 82596761	227	226 : 15
182	27 : 2	228	151 : 10
183	487 : 36	229	1710 : 113
184	24335 : 1794	230	91 : 6
185	68 : 5	231	76 : 5
186	7501 : 550	232	19603 : 1287
187	1682 : 123	233	23156 : 1517
188	4607 : 336	234	5201 : 340
189	55 : 4	235	46 : 3
190	52021 : 3774	236	561799 : 36570
191	8994000 : 650783	237	228151 : 14820
192	97 : 7	238	11663 : 756
193	1764132 : 126985	239	6195120 : 400729
194	195 : 14	240	31 : 2
195	14 : 1	241	71011068 : 4574225
197	14 : 1	242	19601 : 1260
198	197 : 14	243	70226 : 4505
199	16266196520 : 1153080099	244	1766319049 : 113076990
200	99 : 7	245	51841 : 3312
201	515095 : 36332	246	88805 : 5662
202	3141 : 221	247	85292 : 5427
203	57 : 4	248	63 : 4
204	4999 : 350	249	8553815 : 542076
205	39689 : 2772	250	4443 : 281
206	59535 : 4148	251	3674890 : 231957
207	1151 : 80	252	127 : 8
208	649 : 45	253	3222617399 : 202604220
209	46551 : 3220	254	255 : 16
210	29 : 2	255	16 : 1
211	278354373650 : 19162705353	257	16 : 1
212	66249 : 4550	258	257 : 16
213	194399 : 13320	259	847225 : 52644
214	695359189925 : 47533775646	260	129 : 8
215	44 : 3	261	192119201 : 11891880
216	485 : 33	262	104980517 : 6485718
217	3844063 : 260952	263	139128 : 8579
218	251 : 17	264	65 : 4
219	74 : 5	265	6072 : 373
220	89 : 6	266	685 : 42
221	1665 : 112	267	2402 : 147
222	149 : 10	268	4771081927 : 291440214

N	$x : y$	N	$x : y$
269	82 : 5	313	126862368 : 7170685
270	5291 : 322	314	443 : 25
271	115974988600 : 7044978537	315	71 : 4
272	33 : 2	316	12799 : 720
273	727 : 44	317	352618 : 19805
274	1407 : 85	318	107 : 6
275	199 : 12	319	12901780 : 722361
276	7775 : 468	320	161 : 9
277	8920484118 : 535979945	321	215 : 12
278	2501 : 150	322	323 : 18
279	1520 : 91	323	18 : 1
280	251 : 15	325	18 : 1
281	1063532 : 63445	326	325 : 18
282	2351 : 140	327	217 : 12
283	138274082 : 8219541	328	163 : 9
284	24220799 : 1437240	329	2376415 : 131016
285	2431 : 144	330	109 : 6
286	561835 : 33222	331	2785589801443970 :
287	288 : 17		153109862634573
288	17 : 1	332	13447 : 738
290	17 : 1	333	73 : 4
291	290 : 17	334	63804373719695 :
292	2281249 : 133500		3491219999244
293	2482 : 145	335	604 : 33
294	4801 : 280	336	55 : 3
295	2024999 : 117900	337	1015827336 : 55335641
296	3699 : 215	338	239 : 13
297	48599 : 2820	339	97970 : 5321
298	409557 : 23725	340	285769 : 15498
299	415 : 24	341	10626551 : 575460
300	1351 : 78	342	37 : 2
301	5883392537695 :	343	130576328 : 7050459
	339113108232	344	10405 : 561
302	4276623 : 246092	345	6761 : 364
303	2524 : 145	346	93 : 5
304	57799 : 3315	347	641602 : 34443
305	489 : 28	348	1567 : 84
306	35 : 2	349	9210 : 493
307	88529280 : 5052633	350	449 : 24
308	351 : 20	351	62425 : 3332
309	64202725495 : 3652365444	352	77617 : 4137
310	848719 : 48204	353	71264 : 3793
311	16883880 : 957397	354	258065 : 13716
312	53 : 3	355	954809 : 50676

N	$x : y$	N	$x : y$
356	500001 : 26500	401	20 : 1
357	3401 : 180	402	401 : 20
358	176579805797 : 9332532726	403	669878 : 33369
359	360 : 19	404	201 : 10
360	19 : 1	405	161 : 8
362	19 : 1	406	59468095 : 2951352
363	362 : 19	407	2663 : 132
364	4954951 : 259710	408	101 : 5
365	3458 : 181	409	111921796968 : 5534176685
366	907925 : 47458	410	81 : 4
367	19019995568 : 992835687	411	49730 : 2453
368	1151 : 60	412	103537981567 : 5100950232
369	8396801 : 437120	413	113399 : 5580
370	327 : 17	414	24335 : 1196
371	1695 : 88	415	18412804 : 903849
372	12151 : 630	416	5201 : 255
373	5118 : 265	417	85322647 : 4178268
374	3365 : 174	418	33857 : 1656
375	15124 : 781	419	270174970 : 13198911
376	2143295 : 110532	420	41 : 2
377	233 : 12	421	44042445696821418 :
378	8749 : 450		2146497463530785
379	12941197220540690 :	422	7022501 : 341850
	664744650125541	423	4607 : 224
380	39 : 2	424	32080051 : 1557945
381	1015 : 52	425	268 : 13
382	164998439999 : 8442054600	426	88751 : 4300
383	18768 : 959	427	62 : 3
384	4801 : 245	428	1850887 : 89466
385	95831 : 4884	429	1524095 : 73584
386	111555 : 5678	430	2862251 : 138030
387	3482 : 177	431	151560720 : 7300423
388	62809633 : 3188676	432	1351 : 65
389	1282 : 65	433	7230660684 : 347483377
390	79 : 4	434	125 : 6
391	7338680 : 371133	435	146 : 7
392	99 : 5	436	158070671986249
393	46437143 : 2342444		7570212227550
394	395023035 : 19900973	437	4599 : 220
395	159 : 8	438	293 : 14
396	199 : 10	439	440 : 21
397	20478302982 : 1027776565	440	21 : 1
398	399 : 20	442	21 : 1
399	20 : 1	443	442 : 21

N	$x : y$
444	295 : 14
445	4662 : 221
446	110166015 : 5216512
447	148 : 7
448	127 : 6
449	189471332 : 8941705
450	19601 : 924
451	46471490 : 2188257
452	1204353 : 56648
453	1653751 : 77700
454	169160400841175685 : 793909098494766
455	64 : 3
456	1025 : 48
457	59089951584 : 2764111349
458	107 : 5
459	499850 : 23331
460	2535751 : 118230
461	24314110 : 1132421
462	43 : 2
463	247512720456368 : 11502891625161
464	9801 : 455
465	15871 : 736
466	938319425 : 43466808
467	1625626 : 75225
468	649 : 30
469	137215 : 6336
470	1691 : 78
471	7838695 : 361188
472	306917 : 14127
473	87 : 4
474	193549 : 8890
475	57799 : 2652
476	28799 : 1320
477	8777860001 : 401910600
478	1617319577991743 : 73974475657896
479	2989440 : 136591
480	241 : 11
481	964140 : 43961
482	483 : 22
483	22 : 1
485	22 : 1
486	485 : 22
487	51906073840568 : 2352088722477
488	243 : 11
489	7592629975 : 343350596
490	1039681 : 46968
491	93628044170 : 4225374483
492	29767 : 1342
493	683982 : 30805
494	73035 : 3286
495	89 : 4
496	4620799 : 207480
497	1201887 : 53912
498	179777 : 8056
499	4490 : 201
500	930249 : 41602
501	11242731902975 : 502288218432
502	3832352837 : 171046278
503	24648 : 1099
504	449 : 20
505	809 : 36
506	45 : 2
507	1351 : 60
508	44757606858751 : 1985797689600
509	395727950 : 17540333
510	271 : 12
511	4188548960 : 185290497
512	665857 : 29427
513	13771351 : 608020
514	4625 : 204
515	17406 : 767
516	16855 : 742
517	590968985399 : 25990786260
518	2367 : 104
519	14851876 : 651925
520	6499 : 285
521	128377240 : 5624309
522	19603 : 858
523	81810300626 : 3577314675
524	225144199 : 9835470
525	6049 : 264

N	$x : y$
526	84056091546952933775 : 3665019757324295532
527	528 : 23
528	23 : 1
530	23 : 1
531	530 : 23
532	2588599 : 112230
533	6118 : 265
534	3678725 : 159194
535	1618804 : 69987
536	145925 : 6303
537	192349463 : 8300492
538	69051 : 2977
539	3970 : 171
540	119071 : 5124
541	1361516316469227450 : 58536158470221581
542	4293183 : 184408
543	669337 : 28724
544	2449 : 105
545	1961 : 84
546	701 : 30
547	160177601264642 : 6848699678673
548	6083073 : 259856
549	1766319049 : 75384660
550	30580901 : 1303974
551	8380 : 357
552	47 : 2
553	624635837407 : 26562217704
554	174293 : 7405
555	1814 : 77
556	12032115501124999 : 510275358434250
557	118 : 5
558	7937 : 336
559	506568295 : 21425556
560	71 : 3
561	522785 : 22072
562	220938497 : 9319728
563	68122 : 2871
564	95 : 4
565	14752278 : 620633
566	95609285 : 4018758
567	2024 : 85
568	143 : 6
569	2894863832 : 121359005
570	191 : 8
571	181124355061630786130 : 7579818350628982587
572	287 : 12
573	383 : 16
574	575 : 24
575	24 : 1
577	24 : 1
578	577 : 24
579	385 : 16
580	289 : 12
581	152071153975 : 6308974548
582	193 : 8
583	8429543 : 349116
584	145 : 6
585	33281 : 1376
586	4115086707 : 169992665
587	1907162 : 78717
588	97 : 4
589	41423166067036218751 : 1706811823063746000
590	5781 : 238
591	165676 : 6815
592	73 : 3
593	600632 : 24665
594	1098305 : 45064
595	18514 : 759
596	25801741449 : 1056880510
597	463287093751 : 18961078500
598	1574351 : 64380
599	24686379794520 : 1008658133851
600	49 : 2
601	139468303679532 : 5689030769845
602	687 : 28
603	48842 : 1989
604	5972991296311683199 : 243037569063951720
605	930249 : 37820
606	42187499 : 1713750

N	$x : y$	N	$x : y$
607	164076033968:6659640783	646	305 : 12
608	2737 : 111	647	120187368 : 4725053
609	605695 : 24544	648	19601 : 770
610	71847 : 2909	649	1123593226162199 : 44104892095380
611	236926 : 9585	650	51 : 2
612	2177 : 88	651	1735 : 68
613	481673579088618 : 19454612624065	652	8212499464321351 : 321626301297510
614	348291186245:14055888354	653	2291286382 : 89664965
615	124 : 5	654	8915765 : 348634
616	21295 : 858	655	737709209 : 28824684
617	41009716 : 1650989	656	2049 : 80
618	10093 : 406	657	2281249 : 89000
619	5172135105532829930 : 207885661805487339	658	1693 : 66
620	249 : 10	659	5930 : 231
621	7775 : 312	660	1079 : 42
622	13804370063 : 553504812	661	28654544354225833218 : 1114532602963469005
623	624 : 25	662	1718102501 : 66775950
624	25 : 1	663	103 : 4
626	25 : 1	664	1700902565 : 66007821
627	626 : 25	665	13719 : 532
628	46698728731849 : 1863482146110	666	27365201 : 1060380
629	7850 : 313	667	107119097 : 4147668
630	251 : 10	668	56447 : 2184
631	489615753129986500355560 19491295375751510364427	669	142261178559054135 : 5500134926184336
632	7743 : 308	670	5791211 : 223734
633	440772247 : 17519124	671	58620 : 2263
634	65999458125 : 2621173333	672	337 : 13
635	126 : 5	673	48813455293932 1881620424025
636	3505951 : 139020	674	675 : 26
637	1419278889601 : 56233877040	675	26 : 1
638	42283 : 1674	677	26 : 1
639	24220799 : 958160	678	677 : 26
640	1039681 : 41097	679	17792625320 : 682818291
641	36120833468 : 1426687145	680	339 : 13
642	5777 : 228	681	10743166003415 : 411679015748
643	1988960193026 : 78436933185	682	1197901 : 45870
644	11775 : 464	683	170067682 : 6507459
645	1024001 : 40320	684	57799 : 2210

Die Gleichung $x^2 - Ny^2 = -1$ ist stets auflösbar, wenn N eine Primzahl von der Form $4n + 1$ ist; dasselbe gilt noch für unendlich viele andere gerade oder ungerade Werte von N. Im Falle diese Gleichung auflösbar ist, beziehen sich die Zahlen x und y, welche in der Tafel stehen, immer auf die Gleichung $x^2 - Ny^2 = -1$. Nennt man diese Zahlen a und b, so sind $2a^2 + 1$ und $2ab$ die kleinsten Zahlen, welche der Gleichung $x^2 - Ny^2 = +1$ genügen. Man kann übrigens leicht auf den ersten Blick erkennen, ob die in der Tafel stehenden Zahlen der einen oder andern von diesen Gleichungen Genüge leisten; es ergiebt sich dies nämlich unmittelbar, wenn man die Werte von x und y auf ihre letzte Ziffer reduciert.